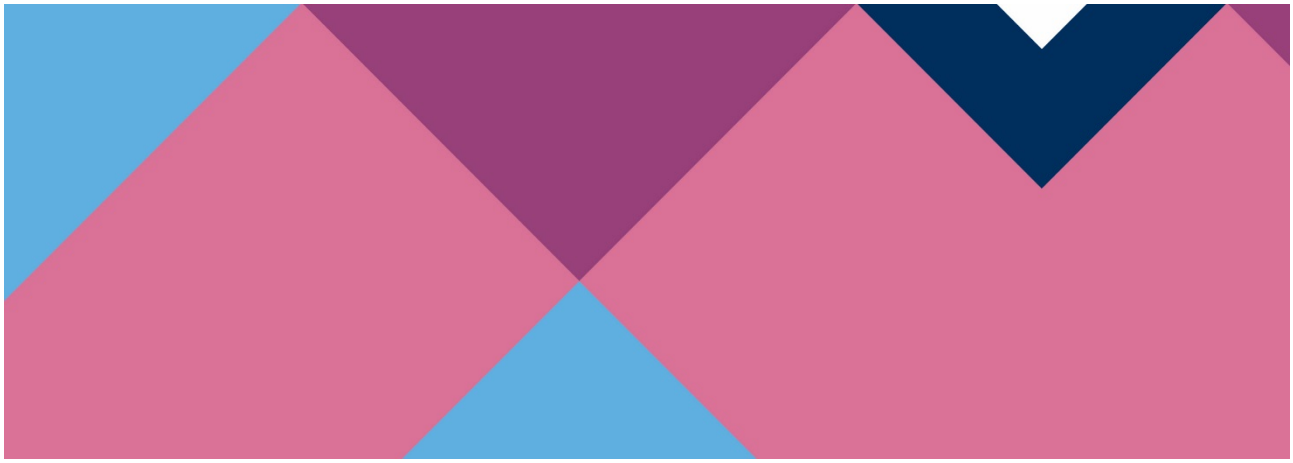
VERIFICATION
VALIDATION
METHODS

Zusammenfassender Abschlussbericht

VVMethoden / Verifikations- und Validierungsmethoden automatisierter Fahrzeuge Level 4 und 5



Version 1.0

Editor Roland Galbas und Mark Schiementz

Projektkoordination Robert Bosch GmbH und BMW AG

Fälligkeit 30.06.2024

Veröffentlichung 26.07.2024

Förderkennzeichen: 19A19002A - 19A19002W

PEGASUS FAMILY

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Dokumenteninformation

Autoren

Adam Bachorek - FhG IESE
Tino Brade - Bosch
Christian Bühler - PROSTEP
Andreas Bussler - Volkswagen
Christopher Deiner - BMW
Martin Dörr - ZF
Ulrich Eberle - Opel/Stellantis
Julian Fuchs - FZI
Roland Galbas - Bosch
Roman Gansch - Bosch
Christoph Glasmacher - ika
Christian Gutenkunst - AVL
Veronika Haber - PROSTEP
Fin Heuer - DLR
Hardi Hungar - DLR
Thomas Kirschbaum - Bosch
Slavisa Krebs-Radic - ZF
Martin Mai - ZF
Jonathan Militzer - FhG LBF
Henning Mosebach - DLR
Christian Müller-Hirschkorn - Valeo
Christian Neurohr - DLR
Jürgen Nuffer - FhG LBF
Stefan Otten - FZI
Hubert Padusinski - FZI
Nikos Papamichail - EICT
Jonas Pfisterer - Valeo
Andreas Pütz - Ford
Tuan Dong Quang - TÜV Süd
Jana Rehbein - Volkswagen
Jan Reich - FhG IESE
Werner Ritter - Mercedes-Benz
Nayel Fabian Salem - TU Braunschweig
Mark Schiementz - BMW
Helmut Schittenhelm - Mercedes-Benz
Michael Schuldes - ika
Alexander Spot - dSPACE
Kai Storms - TU Darmstadt
Gerald Temme - DLR
Sebastian Werr - Mercedes-Benz
Max Zipfl - FZI

Reviewer

Tino Brade - Bosch
Christian Bühler - PROSTEP
Martin Butz - ZF
Martin Dörr - ZF
Björn Filzek - ZF
Roland Galbas - Bosch
Veronika Haber - PROSTEP
Hardi Hungar - DLR
Thomas Kirschbaum - Bosch
Christian Lalitsch-Schneider - ZF
Jürgen Likkei - Mercedes-Benz
Marcus Nolte - TU Braunschweig
Jürgen Nuffer - FhG LBF
Niko Papamichail - EICT
Jana Rehbein - Volkswagen
Jan Reich - FhG IESE
Nayel Fabian Salem - TU Braunschweig
Mark Schiementz - BMW
Helmut Schittenhelm - Mercedes-Benz
Kai Storms - TU Darmstadt
Lukas Westhofen - DLR

Kontakt

Roland Galbas
CC-AD
Robert Bosch GmbH
74232 Abstatt

Email: Roland.Galbas@de.bosch.com

Revisionslog

Version	Datum	Kommentar	Autor	Partner
0.1	Bis 31.05.2024	Erstellung auf Confluence	Autoren und Reviewer siehe oben	Alle Partner
0.2	05.06.-17.06.2024	Überführung in Word-Dokument, Layout, formelles Review	Nikos Papamichail	EICT
03	17.06.-24.06.2024	Vorlage zur Freigabe durch Steuerkreis	Nikos Papamichail	EICT
1.0	27.06.2024	Finalisierung und Erstellung pdf	Nikos Papamichail	EICT

Inhaltsverzeichnis

1 Zusammenfassung 14

2 Übersicht 16

2.1 Aufgabenstellung 16

2.1.1 Aufgabestellung I: Beherrschung der Vielzahl möglicher Szenarien 17

2.1.1.1 Ausgangssituation 17

2.1.1.2 Zusammenfassung Aufgabenstellung I: Beherrschung der Vielzahl möglicher Szenarien. 19

2.1.2 Aufgabenstellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen 19

2.1.2.1 Ausgangssituation 19

2.1.2.2 Ansatz zur Lösung von Aufgabenstellung II in VVMethoden 20

2.1.2.3 Zusammenfassung Aufgabenstellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen 21

2.1.3 Aufgabenstellung III: Nahtloses Testen über alle Testinstanzen 22

2.1.3.1 Ausgangssituation 22

2.1.3.2 Ansatz von Aufgabenstellung III in VVMethoden 22

2.1.3.3 Zusammenfassung technisch/wissenschaftliches Aufgabenstellung III: Nahtloses Testen über alle Testinstanzen. 23

2.2 Voraussetzungen für das Vorhaben 24

2.3 Planung und Ablauf 26

2.3.1 Planung 26

2.3.1.1 Teilprojekte 26

2.3.1.2 Projektphasen 28

2.3.2 Ablauf 29

2.3.2.1 Covid-19 Pandemie 29

2.3.2.2 Rückzug Visteon 29

2.3.2.3 Erweiterung Datenbankkonzept 29

2.4 Stand der Wissenschaft und Technik 30

2.4.1 Legal Frameworks 30

2.4.2 Safety Standards 32

2.4.3 Safety Reports 33

2.4.4 Stand der Technik im Bezug zu den Lösungsansätzen 34

2.4.4.1 Methodik zur Ableitung von System- und Testanforderungen – Bestandteil Ansatz II 35
2.4.4.2 Testprozess – Bestandteil Ansatz II / III 35
2.4.4.3 Model/SW-Testing (MiL/SiL) – Bestandteil Ansatz III 38
2.4.4.4 Gerätetest (HiL) – Bestandteil Ansatz III 40
2.4.4.5 Testen im Fahrzeug – Bestandteil Ansatz III 42
2.5 Zusammenarbeit mit anderen Stellen 42
2.5.1 VDA Leitinitiative autonomes und vernetztes Fahren 43
2.5.2 PEGASUS Projektfamilie 43
2.5.3 Offene Treffen zur Ergebnisverbreitung 45
3 Eingehende Darstellung 46
3.1 Erzielte Ergebnisse 46
3.1.1 Die Gesamtmethode 46
3.1.1.1 Methodischer Rahmen 46
3.1.1.1.1 Aufsatzpunkt PEGASUS 46
3.1.1.1.2 Kernergebnisse und gemeinsame Grundlagen 55
3.1.1.1.3 Standardisierung 58
3.1.1.1.4 Fachsprache 61
3.1.1.2 Methodischer Überblick 62
3.1.1.2.1 Die VVM - Sicherheitsargumentation 89
3.1.1.2.2 Gesellschaftliche Erwartung und Erfüllung der Sicherheit 91
3.1.1.2.3 Hauptkonzept für die Absicherung des Sicherheitsanspruches 94
3.1.1.2.4 Sicherheitsargumentation 97
3.1.1.2.5 Herausforderung Sicherheit-Management automatisierter Fahrsysteme 98
3.1.1.2.6 Strategischer Link zwischen Test & Absicherung und der Sicherheitsargumentation 100
3.1.1.2.7 Concern Management 104
3.1.1.2.8 Traceability und Durchgängigkeit 104
3.1.1.3 Operational Concept / ODD 106
3.1.1.3.1 Was ist eine Kundenfunktion? 106
3.1.1.3.2 Was ist ein Automated Driving System (ADS)? 106
3.1.1.3.3 Operational Design Domain (ODD) 107
3.1.1.3.4 Wieso wird in VVM eine Kundenfunktion benötigt? 107
3.1.1.3.5 Gesetzeslage/ State of the Art: EU Level 4, AFGBV 108
3.1.1.3.6 Regelkonformes Verhalten im Straßenverkehr 109
3.1.1.3.7 Operational Design Domain (ODD) 112
3.1.1.3.8 Top Goals 115

3.1.1.3.9 Das Verfahren 116
3.1.1.3.10 Dekomposition der Fähigkeiten 116
3.1.1.4 Szenarienabstraktion Grundlagen (Realitätsabstraktion) 116
3.1.1.4.1 Die Rolle der "Realitätsabstraktion" in der szenariobasierten Entwicklung eines ADS 116
3.1.1.4.2 Ganzheitliches urbanes Fahrszenario-Konzept 126
3.1.1.4.3 Von Daten zu logischen Szenarien mit Parameterverteilungen 129
3.1.1.4.4 Datenbank mit logischen Stadtverkehrsszenarien 130
3.1.1.4.5 Vorgehen zur Vollständigkeitsargumentation des Szenario Konzepts 131
3.1.1.4.6 Ontologie und OD Beschreibung 134
3.1.1.4.7 Datenbasierte Identifikation von risikobehafteten Szenarien 137
3.1.1.4.8 Motivation 137
3.1.1.4.9 Methode 137
3.1.1.4.10 Ergebnisse 138
3.1.1.4.11 Fazit 140
3.1.1.5 Szenarienabstraktion - Szenariobasiertes Testen 140
3.1.1.5.1 Warum szenariobasierte Tests? 140
3.1.1.5.2 Methoden zur Reduktion und Optimierung des Testaufwands 147
3.1.1.5.3 beim szenariobasierten simulativen Testen der automatischen Funktionalität und Evaluierung des verbleibenden Restrisikos. 147
3.1.1.5.4 Risiko-basierte Auswahl von konkreten Testszenarien für ein CORE Szenario 149
3.1.1.6 Kritikalitätsanalyse 150
3.1.1.6.1 Der Prozess der Kritikalitätsanalyse 150
3.1.1.6.2 Die Teilgebiete der Kritikalitätsanalyse 154
3.1.1.7 Fähigkeitenanalyse und Verhaltensspezifikation 161
3.1.1.7.1 Motivation und Überblick 161
3.1.1.7.2 Semantische Normverhaltensanalyse 163
3.1.1.7.3 Phänomen-Signal-Modell 165
3.1.1.7.4 Verhaltenssicherheitskonzept 166
3.1.1.7.5 Identifikation und Konsolidierung von Systemfähigkeiten 169
3.1.1.8 Requirementsbreakdown zu Design und Validation / Verifikation 171
3.1.1.8.1 Storyline Requirement Flow 171
3.1.1.8.2 Requirements for Test Planning 175
3.1.1.8.3 Requirements for Test Orchestration 176
3.1.1.8.4 Safety-related Quality Measures: From Risk Reduction Need to Design Constraints 177
3.1.1.8.5 Examples for Quality Measures 179

3.1.1.9 V&V-Domäne ... 182
3.1.1.9.1 V&V Domäne - Überblick ... 182
3.1.1.9.2 V&V Konzept ... 188
3.1.1.9.3 Testplanung ... 192
3.1.1.9.4 Testorchestrierung ... 194
3.1.1.9.5 Test execution and evaluation ... 196
3.1.2 Überblick über die VVM-Gesamtmethode ... 199
3.1.2.1 TP1 Rahmenbedingungen und Impulsgeber ... 199
3.1.2.2 TP2 Kritikalitätsanalyse ... 206
3.1.2.2.1 Zusammenfassung der TP2-Arbeiten ... 206
3.1.2.2.2 AP2.1 - Charaktersierung des Szenarienraums und Ontologie für Szenarienannotation ... 206
3.1.2.2.3 AP2.2 - Ermittlung von kritikalitätsbeeinflussenden Wirkzusammenhängen und Szenarienerzeugung ... 216
3.1.2.2.4 AP2.3 - Sicherheitsprinzipien und Gesamtmethodik Kritikalitätsanalyse ... 224
3.1.2.2.5 AP2.4 - Ermittlung Güteanforderungen Sensorik ... 225
3.1.2.3 TP3 Sicherheitsbewertung und -konzept ... 229
3.1.2.4 TP4 Regelwerk System - und Testanforderungen ... 231
3.1.2.4.1 Goal – Question – Metric (GQM) ... 231
3.1.2.4.2 Sicherheitsanalyse von (Un-)Fähigkeiten und Schwachstellen mit Component Fault Trees und probFMEA ... 233
3.1.2.4.3 Anforderungen für die Testplanung ... 237
3.1.2.4.4 Testplanung ... 239
3.1.2.5 TP5 Simulationssteuerung ... 243
3.1.2.5.1 AP5.1 Anforderungen an die Simulationstechnologie ... 243
3.1.2.5.2 AP5.2 Verfügbarmachung und Instanziieren einer Simulationsumgebung ... 247
3.1.2.6 TP6 Datenbereitsstellung ... 250
3.1.2.6.1 HD Kartenerstellung für Ground Truth Daten ... 250
3.1.2.6.2 Datenreduktion ... 252
3.1.2.6.3 Datenaufzeichnungsprozess ... 255
3.1.2.6.4 Durchgängiges Beispiel ... 258
3.1.2.7 TP7 Testvorgehen ... 261
3.1.2.7.1 Testprozess ... 262
3.1.2.7.2 Durchgängiges Testen ... 267
3.1.2.7.3 Exemplarische Realisierungen ... 269
3.1.2.8 TP8 Datenbank ... 301
3.1.2.8.1 Einleitung ... 301

3.1.2.8.2 Szenariendatenbank ... 301
3.1.2.8.3 Ausspielung von Szenarien ... 305
3.1.2.8.4 Entwicklungsdatenbank ... 308
3.1.2.8.5 Aufnahme von Referenzdaten ... 308
3.1.2.8.6 Verwaltung von Referenzdaten ... 309
3.1.2.8.7 Zusammenfassung ... 310
3.1.2.9 TP9 Prozess Instanziierung, Anwendung ... 312
3.1.2.9.1 Zielsetzung ... 312
3.1.2.9.2 Anforderungserhebung ... 313
3.1.2.9.3 Unterstützung für die Instanziierung ... 324
3.1.2.9.4 Die Gesamtmethode im SysML-Modell ... 327
3.1.2.9.5 Abbildung der Gesamtmethode im Traceability Demonstrator ... 342
3.1.2.9.6 Zusammenfassung und weiteres Vorgehen ... 351
3.1.2.10 TPX ... 352
3.1.2.10.1 Executive Summary Abschlussbericht Teilprojekt VVM-TPX ... 352
3.1.2.10.2 2 Ergebnisse der Arbeitsgruppen von VVM-TPX ... 355
3.1.2.10.3 Ausblick auf thematische Zukunftsfelder über VVM hinaus ... 365
3.2 Nutzen und Verwertbarkeit ... 370
3.3 Projekt Impact ... 371
4 Veröffentlichungen ... 378
5 Abbildungsverzeichnis ... 383
6 Tabellenverzeichnis ... 394
7 Literaturverzeichnis ... 395
1 ANNEX I - VVM Position Papier ... 1
1.1 Introduction ... 1
1.1.1 Executive summary ... 1
1.1.2 Status VV Methods and scenario-based safety assurance ... 3
1.1.3 VVM goals, challenges and solution space ... 4
1.2 The VV Methods position by theses and argumentation ... 7
1.2.1 Subthesis 1 – Consistent usage of an ODD Metamodel Approach ... 7
1.2.2 Subthesis 2 – Mastering complexity by safety-by-design-approach ... 9
1.2.3 Subthesis 3 – The Risk Management Core ... 10
1.2.4 Subthesis 4 – The VVM Safety argumentation ... 11
1.3 VVM solution structure ... 13
1.3.1 Global Development and V&V perspective ... 15

1.3.2 Scenario-based Development and Testing perspective 16
1.3.3 Risk Management Perspective 17
1.3.4 Safety Argumentation Perspective 18
1.3.5 Enabler, Premises and Summary of Solution 19
1.4 Conclusions, recommendations and future perspectives 19
1.4.1 Outlook: Scenario-based testing and virtualization 20
1.4.1.1 Upscaling critical scenarios 20
1.4.1.2 Application of ODD modeling 20
1.4.1.3 Reality abstraction, virtual environments and corresponding tooling 20
1.4.1.4 Innovative data- and data-service ecosystems 20
1.4.1.5 Updated and harmonized scenario DBs 21
1.4.2 Outlook: Risk Handling and safety case application 21
1.4.2.1 Application of risk modeling 21
1.4.2.2 The role of risk management for Security / Cybersecurity 21
1.4.2.3 Applying the safety case on concrete ODDs 22
1.4.3 Outlook: Technological Challenges 22
1.4.3.1 Explicit Specification of Target Behavior 22
1.4.3.2 The role of AI in the safety case 22
1.4.3.3 Concernmanagement 23
1.4.3.4 Remote Operation 23
1.4.3.5 Collective learning and adjustment concepts from in-field operations 23
1.5 Epilogue: Product driven safety assurance 24

Abkürzungsverzeichnis

Abkürzung	Bedeutung
6LM	6-Layer-Modell
AD	Automatisiertes Fahrsystem
ADAS	Advanced Driver Assistance System
ADF	Automated Driving Function
ADS	Automated Driving System
AF	Automatisierte Fahrsysteme
AFGBV	Automatisiertes Fahren Genehmigungs- und Betriebsverordnung
ARtS	Advanced Replay to Simulation
ASAM	Association for Standardization of Automation and Measuring Systems
ASE	Szenarien-Identifikations-Algorithmik
ASIL	Automotive Safety Integrity Level
ASM	Automotive Simulation Models
AUTO	Automotive Urban Traffic Ontology
AVP	automatisiertes Valet-Parking
BN	Bayes‘sche Netze
BSR	Behavioral Safety Requirements
CADR	Context Aware Data Reduction
CFT	Component Fault Trees
COD	Current Operational Domain
CP	Criticality Phenomenon
CR	Causal Relation
CSCC	Continuous Shift-Left Convergence Concept
DDI	Digital Dependability Identity
DDT	Dynamic Driving Task
FAS	Fahrerassistenzsystem
FOT	Field Operational Test
FUC	Functional Use Case
GAN	Generative Adversarial Networks

GDPR	General Data Protection Regulation
GQM	Goal Question Metric
GT	Ground Truth
HARA	Hazard Analysis and Risk Assessment
HiL	Hardware-in-the-Loop
IMU	Inertial Measurement Unit
ISRQB	International Software Testing Qualifications Board
JSON	JavaScript Object Notation
KF	Kundenfunktion
KPI	Key Performance Indicators
MBSE	Modellbasiertes Systems Engineering
MoSAIC	Modular and Scalable Application Platform for ITS Component
MOTA	Multiple Object Tracker Accuracy
OD	Operational Domain
ODD	Operational Design Domain
ODE	Open Dependability Exchange
OSI	Open Systems Interconnection
OWL	Web Ontology Language
PCD	Point Cloud Data
PRB	Positive Risikobilanz
probFMEA	probabilistische Fehlermöglichkeits- und Einflussanalyse
PSM	Phänomen-Signal-Modell
RAW DB	Rohdatenbank
RMC	Risk Management Core
RTK-GNSS	Real-Time Kinematic - Global Navigation Satellite Systems
RtS	Replay to Simulation
SACRED	Structured Analysis for Conservative Relevance Estimation in Driving context
SiL	Software in the Loop
SOCA	Scode for Open Context Analysis
SOTIF	Safety of the intended Functionality

StVG	Straßenverkehrsgesetzes
StVO	Straßenverkehrsordnung
STVZO	Straßenverkehrszulassungsordnung
SUT	System under Test
SysML	Systems Modeling Language
TLE	Top-Level-Element
TOD	Target Operational Domain
TT	technische Testspezifikation
UC	Use Case
VCIP	Virtual Continuous Integration Platform
ViL	Vehicle-in-the-Loop
VLSS	Vehicle-Level SOTIF Strategy
VRU	Vulnerable Road User
WGS84	World Geodetic System 1984

1 Zusammenfassung

Mit VVMethoden geht ein für die deutsche Automobilindustrie wichtiges Projekt zu Ende, in dem zentrale Ergebnisse für die Entwicklung von sicherem und akzeptierten automatisiertem Fahren erarbeitet wurden.

Je höher der Grad beim automatisierten Fahren und je komplexer das Einsatzgebiet eines Systems, desto mehr Faktoren müssen bei der Entwicklung berücksichtigt werden. Es wurden bereits erste SAE Level 3-Systeme für das Autobahnfahren und ein SAE Level 4-System für das fahrerlose Parken zugelassen. Für eine Ausweitung auf weitere Einsatzgebiete – wie dem Stadtverkehr – steigen die Komplexität und die Anforderungen an Fahrzeug und System deutlich an. Aus diesem Grund sind entsprechend geeignete Verifikations- und Validierungsmethoden notwendig, deren Entwicklung im Fokus dieses großen Verbundprojektes stand.

Das vom Bundesministerium für Wirtschaft und Klimaschutz geförderte und von der VDA Leitinitiative autonomes und vernetztes Fahren initiierte vorwettbewerbliche Forschungsprojekt hat 21 Partner zusammengeführt um die weltweit ersten Strukturen zu entwickeln, mit denen Sicherheitsstandards bei automatisierten Fahrzeugen im urbanen Umfeld nachweisbar gemacht werden können.

Herausforderung Stadtverkehr

Eine der größten Herausforderung beim automatisierten Fahren im Beherrschen des Verkehrs im urbanen Umfeld mit zum Beispiel Fußgängern, Radfahrern, motorisierten Zweirädern oder schwer einsehbaren Straßenkreuzungen. Neben der Diversität der Verkehrsteilnehmer ist das Umfeld oft auch durch eine hohe Anzahl von Verkehrsteilnehmern, Ampelsystemen, Verkehrszeichen und Fahrzeugen geprägt. Um diese Komplexität und dabei auch höchst seltene Szenarien beherrschbar zu machen, werden nachvollziehbare Strukturen und Prozesse benötigt, die den sicheren Betrieb eines Systems auch in Ausnahmesituationen einerseits ermöglichen. Andererseits muss auch die Nachweisbarkeit sichergestellt werden, dass die Fahrzeuge in diesem Umfeld sicher manövrieren können, auch um die nötige Akzeptanz gegenüber autonomen Fahrfunktionen in der Bevölkerung herzustellen. Und diese Nachweisbarkeit der Zuverlässigkeit muss bereits in der Entwicklung dieser Systeme beginnen.

Voraussetzung für Verkehrszulassung: Nachweisbare Sicherheit

Bereits bei der Auslegung und Entwicklung von automatisierten Fahrfunktionen muss der Sicherheitsgrundsatz an erster Stelle stehen. Entsprechend müssen diese Sicherheitsfunktionen für die Verkehrszulassung eines Fahrzeuges und einer zertifizierten Freigabe für den Straßenverkehr nachgewiesen werden. Um diesen Nachweis erbringen zu können, wurde in VVMethoden ein Modell erarbeitet, das aus verschiedenen Verfahren, Methoden und Werkzeugen besteht.

Einer der zentralen Ansätze zum Nachweis der Sicherheit lag im stringenten Herunterbrechen und Zusammenführen gesellschaftlicher Ansprüche und deren Abbildung auf das gesamte Fahrzeug-System. Anforderungen wurden also einerseits auf das Design – die linke Seite des V-Modells – heruntergebrochen und andererseits auf die technische Prüfung – die rechte Seite des V Modells. Diese kohärente Anforderungssystematik ermöglicht nicht nur eine adäquate Prüfung des Systems, sie bildet gleichzeitig die Grundlage für „Safety by Desing“. Die dadurch zudem entstehende Rückverfolgbarkeit von Anforderungen ermöglicht Effizienz für die Prüfung des

Systems aber auch für z.B. Designänderungen. Mit der im Projekt entwickelten Sicherheitsargumentation kann der Nachweis erbracht werden, dass das System sicher nutzbar ist. Die stringente Systematik einer Sicherheitsargumentation erlaubt einerseits Zertifizierungsorganisationen als auch domänenfremden Stakeholdern wie Rechtsvertreten einen verbesserten Zugang. Nicht zuletzt wurde auf bestehenden Standards aufgebaut und damit die Anschlussfähigkeit der Industrie erhöht.

Für die methodische Ausgestaltung dieses Modells haben die Partner in 9 Teilprojekten zusammengearbeitet um die Grundlage zu schaffen, die Sicherheit in automatisierten Fahrzeugen nachzuweisen. Durch die offene Ergebnisverbreitung – nicht zuletzt im Rahmen des vorliegenden, öffentlichen Abschlussberichts – stehen diese erarbeiteten Modelle branchenweit zur Verfügung und ermöglichen es erstmals, dass allen Automobilherstellern dieselben Strukturen bei der Verifikation und Validierung automatisierter Fahrsysteme im städtischen Umfeld zur Verfügung stehen. Diese Vereinheitlichung könnte dann auch in industrieweite Standards münden, die den Straßenverkehr für alle Verkehrsteilnehmer noch sicherer machen können.

VVMethoden als Technologie-Vorreiter

Der methodische Ansatz aus dem VVM-Projekt ist weltweit das erste Konzept, das auch industrielle Prozesse berücksichtigt. Damit macht sich die deutsche Automobilindustrie erneut zum technologischen Vorreiter beim automatisierten Fahren. Bereits im Jahr 2021 trat mit einem entsprechenden Gesetz in Deutschland die weltweit erste Regulierung für vollautomatisiertes Fahren (SAE Level 4) in Kraft. In 2022 wurde eine entsprechende Verordnung mit den technischen Details beschlossen, um entsprechende Fahrzeuge auf deutschen Straßen zulassen und betreiben zu können. Somit setzt die deutsche Autoindustrie einmal mehr an der Komplexität des automatisierten Fahrens an und macht sie beherrschbarer.

Am Ende seiner Projektlaufzeit und aufbauend auf den Ergebnissen der Vorgängerprojekte Pegasus und SetLevel liefert VVM somit erstmals einen durchgängigen methodischen Sicherheitsansatz für automatisiertes Fahren im urbanen Umfeld, mit dem eine branchenweite Zusammenarbeit und Wertschöpfung möglich wird. Der im Projekt verfolgte Ansatz des szenarienbasierten Sicherheitsnachweises könnte nach behördlicher Zustimmung helfen, weltweite Standards zu setzen. VVM hat ein für die Branche zukunftsrelevantes Referenzsystem geschaffen, das eine methodische Lücke für die praktische Absicherung schließt und die Vorreiterrolle der deutschen Industrie im internationalen Wettbewerb beim automatisierten Fahren festigt.

2 Übersicht

2.1 Aufgabenstellung

Das Gesamtziel des Projektes war die Entwicklung von Systematik und Methoden für den Sicherheitsnachweis von vollautomatisierten und fahrerlosen Fahrfunktionen und Fahrzeugen (Level 4/5 nach VDA-Definition [1]) zur Homologation im urbanen Umfeld.

Klassische Absicherungsmethoden beruhen vielfach auf der Annahme, dass neue Funktionen hinreichend sicher sind, wenn sie unter Realbedingungen über hunderttausende Kilometer ohne Probleme funktioniert haben ("distanzbasiert"). Dieser Ansatz lässt sich nicht auf L4/L5 Systeme übertragen: Die Extrapolation herkömmlicher Absicherungsmethoden erfordert für ein vollautomatisiertes System, dass ein ausreichender Umfang von Kombinationen konkreter Verkehrssituationen, Umfeldfaktoren und Systemzuständen einschließlich Systemfehlern vollständig betrachtet wird. Der dadurch entstehende Kombinationsraum ist so groß, dass eine statistisch hinreichend vollständige Untersuchung mit aktuell etablierten Testmethoden nicht wirtschaftlich darstellbar ist. Zudem sind die für die Freigabeargumentation des Systems relevanten Situationen / Szenarien nicht vollumfänglich bekannt (Vollständigkeitsdilemma).

Die dem Projekt zugrunde liegende Annahme war, dass diese technisch/wissenschaftlichen Aufgabenstellungen gelöst werden können, indem zunächst der für den Sicherheitsnachweis ausreichende Kombinationsraum (Topologie, Verkehrssituation, Wetter,...) über eine strukturierte Analyse durch eine handhabbare Anzahl von Szenarien darstellbar wird. Diese Szenarien müssen dabei

1. alle statistisch sicherheitsrelevanten Ereignisse umfassen,
2. so beschrieben sein, dass sie für menschliche Experten verständlich sind, da diese die Freigabe erteilen und deswegen verstehen müssen. Und die Szenarien müssen
3. die Vielzahl der tatsächlich vorkommenden und denkbaren Szenarien in einer handhabbaren Anzahl von parametrierten Szenarien zusammenfassen.

Würden alle notwendigen Prüfungen eines L4/L5-Fahrzeuges nur auf Basis von Gesamtfahrzeugtests durchgeführt, entstünde ein gigantischer physischer Prüfaufwand und entsprechender Zeitaufwand [2]. Um den Test- und Freigabeaufwand in einem wirtschaftlichen Rahmen zu gestalten, ist es daher notwendig die Vielzahl notwendiger Szenarien Tests möglichst effektiv & effizient auf geeignete Testinfrastrukturen auch von Sub-Systemen des Gesamtfahrzeugs zu verlagern.

Um die ökonomische und realistische Durchführbarkeit zu erhalten, muss der Sicherheitsnachweis Tests und Testergebnisse unterschiedlicher Testinfrastrukturen und Integrationsstufen (Komponente bis System) nachvollziehbar zusammenführen. Zudem sind neuartige Testbeschreibungen sowie Metriken zur Bewertung der Systeme zu entwickeln, zum Beispiel um eine Sicherheitsargumentation über die Betrachtung von Szenarien führen zu können. Da ein Teil der dann durchzuführenden Tests softwarebasierte Komponenten betreffen können diese mittels Simulationen durchgeführt werden. Für den Sicherheitsnachweis ist dann eine Kombination aus Simulations- und Realtests zu erarbeiten, durch die Testaufwände mit Hilfe von Simulationstechnologien zunehmend in die virtuelle Welt verschoben werden können.

Vor diesem Hintergrund und der Gesamtzielsetzung – der Entwicklung von Systematik und Methoden für den Sicherheitsnachweis von vollautomatisierten und fahrerlosen Fahrfunktionen und Fahrzeugen (Level 4/5 nach VDA-Definition [1] zur Homologation im urbanen Umfeld – wurden drei zentrale technisch/wissenschaftlichen Aufgabenstellungen abgeleitet, die im Projekt bearbeitet wurden:

Aufgabestellung I: Beherrschung der Vielzahl möglicher Szenarien.

Aufgabestellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen

Aufgabestellung III: Nahtloses Testen über alle Testinstanzen.

2.1.1 Aufgabestellung I: Beherrschung der Vielzahl möglicher Szenarien

2.1.1.1 Ausgangssituation

Bisher fährt der Mensch selbst – typischerweise risikomindernd. Vom Grundsatz her hat der Mensch in allen Situationen die Kontrolle über die Fahrfunktionen inne. Für die Entwicklung von Sicherheitsnachweisen greift heute insbesondere die ISO 26262, mit der im Wesentlichen zu zeigen ist, dass elektrische und elektronische Komponenten hinreichend frei von Fehlfunktionen sind, damit der Mensch in allen Situationen die sichere Kontrolle über das Fahrzeug hat.

In vollautomatisierten Fahrzeugen ist der Mensch nicht mehr als (rechtzeitige) Rückfallebene verfügbar. Der Verhaltensanspruch ist somit, dass die Automation selbst alle potentiellen Fahrsituationen und Einflussfaktoren sicher behandeln muss. Der Sicherheitsnachweise für vollautomatisierte und fahrerlose Fahrzeuge muss also nachweisen, dass die Automation in einem ausreichend großen Teil der möglichen Fahrsituationen sicher und risikomindernd agiert.

Wie eingangs erläutert, gibt es eine unüberschaubar große Menge von Szenarien, deren Prüfung und Untersuchung mit herkömmlichen Mitteln einen unbeherrschbaren Aufwand fordert. Noch schwieriger ist es, diese Szenarien korrekt zu definieren und den Nachweis ihrer statistischen Relevanz / Vollständigkeit zu führen. Somit ergab sich die erste technisch/wissenschaftliche Aufgabenstellung für VVMethoden (Aufgabenstellung I):

Aufgabestellung I: Beherrschung der Vielzahl möglicher Szenarien.

Welches sind die sicherheitsrelevanten Verhaltensansprüche an Fahrzeuge im urbanen Verkehr und wie können diese so erfasst werden, dass sie umfassend und gleichzeitig effizient getestet werden können?

Ansatz zur Beantwortung von Aufgabenstellung I in VVMethoden

Um sich dem Problem zu nähern, wurde betrachtet, wie Menschen als Fahrer heute diese Herausforderung meistern: Menschen erlernen in der Fahrschule hinreichend viele Fahrsituationen (Straßentopologien, andere Verkehrsteilnehmer – Position, Geschwindigkeit, vermutliches Verhalten in den nächsten 5-10 Sekunden – Schilder, Verkehrsregeln, etc.) einzuschätzen und Strategien, um diese Fahrsituationen risikokontrollierend zu beherrschen. Dabei lernt der Mensch implizit, Fahrsituationen, die ähnliches Fahrverhalten erfordern, in endlich viele Klassen (<100) einzuteilen.

Die Klassen von Fahrsituationen werden vom Menschen um endlich viele äußere Einflussfaktoren ergänzt, die Risiken beeinflussen wie zum Beispiel Witterung, Sichtverhältnisse,

Straßenbeschaffenheit, Verkehrsteilnehmer die Verkehrsregeln unbeabsichtigt oder mit Absicht verletzen, Einsatzfahrzeuge. Der Mensch passt in Abhängigkeit dieser Einflussfaktoren seine Fahrstrategien für die jeweilige Klasse an zum Beispiel Reduzierung der Geschwindigkeit bei eingeschränkter Sicht. Dieses Wissen wird durch Erfahrungen vertieft und gefestigt. Der Mensch lernt Fahrsituationen kontextabhängig über grundlegende Wirkzusammenhänge in Klassen einzuteilen und risikominimierende Fahrentscheidungen zuzuordnen. Er nutzt dieses implizite Wissen über Klassen von Fahrsituationen und Einflussfaktoren, um immer neue Verkehrssituationen einzuschätzen.

Klassen von Fahrsituationen, Einflussfaktoren und grundlegenden Wirkzusammenhängen sind ein wirkungsvolles, handhabbares Ordnungsprinzip für sicheres Fahren in der Menge aller möglichen Verkehrsszenarien. Gelingt es, das Prinzip der Klassenbildung, Einflussfaktoren und grundlegende Wirkzusammenhänge zu übertragen, kann man im Wesentlichen alle Fahrsituationen, auch solche die in exakt der Form noch nie erlebt wurden, beherrschen und die zugehörigen Sicherheitsprinzipien sowie Fahrmanöver (z.B. Geschwindigkeitsreduktion, Ausweichen) hinreichend sicher ausführen.

VVMethoden hat genau diesen Ansatz verfolgt und über das o.g. Ordnungsprinzip die Vielzahl möglicher Fahrsituationen in beherrschbar viele Klassen eingeteilt. Diese wurden dann mittels repräsentativer Szenarien beschrieben. Zusätzlich wurden von den Szenarien unabhängige Einflussfaktoren ermittelt und beschrieben, darauf aufbauend wurde analysiert, wann Einflussfaktoren und Szenarien eine kritische Kombination ergaben, die beherrscht werden mussten. In der Folge wurden dann Sicherheitskonzepte zur Unfallvermeidung und repräsentative Tests abgeleitet.

Ansatz I: Entwicklung einer Methodik zur handhabbaren Reduktion des L4/L5-Testraums.

- Kritische Situationen und Gefährdungen identifizieren;
- Ableiten der Sicherheitsanforderungen einschließlich einer Definition für normatives Fahrverhalten;
- Fokussierung des Testraumes durch Ableitung repräsentativer Tests.

VVMethoden hat mit diesem Vorgehen drei Ziele erreicht:

1. Erzeugung eines tiefgehenden Verständnisses der relevanten Wirkzusammenhänge in Verkehrsgefährdungen und eine systematische Zuordnung von existierenden Sicherheitsprinzipien und Sicherheitskonzepten inklusive des Nachweises, dass Wirkzusammenhänge hinreichend genau beschrieben werden konnten.

2. Schaffung einer Gesamtmethodik inklusive einer Abdeckungsmetrik für die Entwicklung eines Szenarienkataloges, der die analysierten Wirkzusammenhänge – gemäß der Abdeckungsmetrik – statistisch hinreichend beschreibt und aus dem sich systematisch Testfälle für die Freigabe von L4/L5 Fahrfunktionen ableiten lassen.

3. Darstellung eines repräsentativen Szenarienraumes inklusive einer semantischen Annotation des Szenarienraumes auf Basis der Ontologie für Klassifizierung, Einflussfaktoren und Ermittlung der Wirkzusammenhänge aus (1) und (2).

Im Projektverlauf wurden die für den Use Case Urbane Kreuzung relevanten Wirkzusammenhänge identifiziert. Die Identifikation und der Nachweis aller für das hochautomatisierte urbane Fahren relevanten Wirkzusammenhänge konnte aufgrund der Fokussierung auf den Use Case Urbane Kreuzung nicht in diesem Projekt erfolgen.

2.1.1.2 Zusammenfassung Aufgabenstellung I: Beherrschung der Vielzahl möglicher Szenarien.

Aufgabenstellung I: **Beherrschung der Vielzahl möglicher Szenarien.**	
Ansatz	Ergebnisse
Entwicklung einer Methodik zur handhabbaren Reduktion des L4/L5-Testraums: • Ermittlung und Beschreibung der Klassen mittels repräsentativer, generischer Szenarien; • Ermittlung und Beschreibung der Einflussfaktoren; • Analyse der Wirkzusammenhänge; • systematische Ermittlung kritischer Situationen und Gefährdungen; • Identifikation / Ableitung zugehöriger Sicherheitskonzepte zur Unfallvermeidung; • Ableitung einer handhabbaren Menge repräsentativer, einhüllender Tests.	**I.1**: Darstellung eines repräsentativen Szenarienraumes und Entwicklung einer Ontologie für Klassifizierung, Einflussfaktoren und Entwicklung der Wirkzusammenhänge **I.2:** Identifikation und tiefgehendes Verständnis der relevanten Wirkzusammenhänge in Verkehrsgefährdungen und systematische Zuordnung von Sicherheitsprinzipien und Sicherheitskonzepten. **I.3:** Gesamtmethodik inklusive Abdeckungsmetrik für die Entwicklung von standardisierbaren, hinreichend vollständigen Szenarienkatalogen

2.1.2 Aufgabenstellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen

2.1.2.1 Ausgangssituation

Die Summe der Testanforderungen an L4/L5-Fahrzeuge wird trotz der oben skizzierten Reduktionen gegenüber den heutigen Tests signifikant ansteigen. Gleichzeitig steigt die Komplexität der Systeme an. Um wettbewerbsfähig zu bleiben, müssen Hersteller deswegen zukünftig in der Lage sein, erhobene Testergebnisse und Sicherheitsnachweise wiederzuverwenden und Komponenten bzw. Subsysteme unterschiedlicher Zulieferer zusammenzuführen – ohne Brüche in der Test- und Sicherheitsargumentation für das Gesamtsystem. Für die Freigabe des Gesamtfahrzeugs hat daher die Art der Absicherung von Komponenten und Subsystemen eine zentrale Bedeutung. Die zentrale Forschungsfrage zum technisch/wissenschaftlichen Aufgabenstellung II war also:

Aufgabenstellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen.

Wie können Testmittel und -ergebnisse wiederverwendet bzw. systematisch aggregiert werden, wie können Hersteller und Zulieferer getestete Systeme sowie Tests austauschen und wie kann die Testbarkeit der Sicherheit von Anfang an in das System designed werden?

2.1.2.2 Ansatz zur Lösung von Aufgabenstellung II in VVMethoden

VVMethoden begegnete Aufgabenstellung II indem die Sicherheitsziele des Systems auf allen Systemebenen von Anfang an im Systemdesign berücksichtigt wurden und somit in das System „hinein designed“ wurden, mit dem Ziel, dass resultierende Testanforderungen auf unterschiedlichste Kombinationen von Komponenten passen und zuverlässig sowie effizient umsetzbar und kombinierbar waren.

Auf Basis der Ergebnisse von Aufgabenstellung I wurden globale Sicherheitsziele der L4/L5-Fahrzeuge in Sicherheitsziele auf Subsystem- und Komponentenebene entlang einer generischen funktionalen Architektur heruntergebrochen, nachfolgend wurden System- und Testanforderungen für Subsysteme und Komponenten abgeleitet. Die entwickelten Testkonzepte mussten dabei handhabbar und passend für den Einsatz in einer durchgängig Test- und Wertschöpfungskette zwischen Zulieferern und OEMs sein.

Zur Erreichung von Aufgabenstellung II hat VVMethoden folgenden Ansatz angewendet:

Ansatz II: Entwicklung einer Absicherungsmethodik über alle Systemebenen, die hierarchisch heruntergebrochen werden kann auf die System- und Testanforderungen für verschiedene (Teil-) Komponenten.

- Transformation von Sicherheitskonzepten in Systemanforderungen.
- Strukturierte Anforderungsdefinition an Systeme
- Entwicklung einer Referenzarchitektur mit verbindlichen Schnittstellen und und definierten Integrations- und Absicherungsprozessen

Die Aufgaben bzw. funktionalen Anforderungen an ein automatisiertes Fahrzeug können vereinfacht als „*Erkennen*“ → „*Verstehen/Planen*“ → „*Handeln*“ zusammengefasst werden. Eine passende funktionale Architektur würde dann die funktionalen Komponenten bzw. Subsysteme *Perzeption* → *Verhaltensplanung* → *Aktuation* beinhalten. Diese Architektur ist unabhängig von z.B. Geschwindigkeit oder Verkehrssituation. Die zentralen Sicherheits-, System- und Testanforderungen an Subsysteme und Komponenten können entlang solch einer generischen funktionalen Architektur beschrieben werden.

Ausgehend vom o.g. Ansatz zur Beantwortung von Aufgabenstellung I (der Entwicklung einer Methodik zur handhabbaren Reduktion des L4/L5-Testraums) wurden konkretisierte Verhaltensansprüche bzw. Sicherheitsanforderungen an das Gesamtfahrzeug gestellt, z.B. „in bestimmten Situationen bremsen“. Diese Gesamtsystem-Sicherheitsanforderungen wurden gemäß dem Ansatz zur Erreichung von Aufgabenstellung II (der Entwicklung einer Absicherungsmethodik über alle Systemebenen, die hierarchisch auf die System- und Testanforderungen für verschiedene (Teil-) Komponenten heruntergebrochen werden) mittels Engineering Methoden entsprechenden Sicherheits- und Systemanforderungen der Komponenten der funktionalen Architektur vollständig zugeordnet. Zum Beispiel erfolgte „Situation erkennen“ in → Perzeption, „Verstehen, Planen und Entscheiden“ in → Verhaltensplanung, und die physische Aktuation „Bremsen“ erfolgte im → Bremsaktuator.

Basierend auf dem Ansatz zur Erreichung von Aufgabenstellung II konnte wiederum über Engineering Methoden und über eine strukturierte und durchgehende Sicherheitsargumentation ein Herunterbrechen von Systemanforderungen und Testanforderungen entwickelt bzw. abgeleitet werden. Eine effektive Nutzung des Ansatzes ergab sich dann, wenn die Sicherheitsargumentation des Fahrzeuges nahtlos auf der Sicherheitsargumentation der Komponenten und Subsysteme der funktionalen Architektur aufgebaut werden konnte.

Eine weitere wesentliche Anforderung an praxistaugliche Tests bestand in der Entwicklung von zugehörigen Testmaßen und -kriterien. Diese können grundsätzlich aus den Verhaltensansprüchen abgeleitet werden, also z.B. ob, wie stark oder wann genau gebremst werden muss in verallgemeinerter Form z.B. über die Zeit bis zu Kollision (ttc). Da die Verhaltensansprüche aus dem Ansatz zur Erreichung von Aufgabenstellung I u.a. aus den Risiken des Verkehrskontextes abgeleitet worden sind, war es möglich, risikobasierte Maßstäbe und Kriterien zu entwickeln, die die Grundlage waren, um zu entscheiden ob ein Test „bestanden“ ist oder nicht. Durch die Schaffung von gegenseitig anerkannten Prozessen und Schnittstellen konnte ein realer Einsatz in der Folge gewährleistet werden.

Über das Herunterbrechen von Testanforderungen auf tiefere Systemebenen konnte die Komplexität und der Testaufwand schon während der Designphase abgeschätzt werden. Diese Fähigkeit wurde genutzt, um schon während des Designs die Testbarkeit praxistauglich zu berücksichtigen.

Als Resultat aus dem Vorgehen nach dem hier vorgestellten Ansatz II hat VVMethoden auf Basis einer Sicherheitsargumentation folgende Ergebnisse erarbeitet:

(1) Methoden zur Ableitung von Sicherheitsanforderungen auf System/Sub-Systemen/Komponenten-Ebene aus den Sicherheitsanforderungen auf Fahrzeugebene.

(2) Eine strukturierte Anforderungsdefinition an Systeme und Tests sowie die Definition eines neuartigen Testprozesses und Testvorgehens für die Absicherung von Level4/5-Systemen die Traceability, Nachvollziehbarkeit und Vergleichbarkeit von Testergebnissen über den gesamten Testprozess hinweg ermöglicht.

(3) Metriken und Bewertungskriterien zur Freigabe von Level4/5-Systemen als Vorbereitung für die Standardisierung von Freigabetests für Level4/5-Systeme.

2.1.2.3 Zusammenfassung Aufgabenstellung II: Inkrementelles Testen von Subsystemen und Gesamtsystemen

Aufgabenstellung II: **Inkrementelles Testen von Subsystemen und Gesamtsystemen**	
Ansatz	Ergebnisse
Entwicklung einer Absicherungsmethodik über alle Systemebenen, die hierarchisch auf die System- und Testanforderungen für verschiedene (Teil-) Komponenten heruntergebrochen werden kann.	**II.1:** Methoden zur Ableitung von Sicherheitsanforderungen auf System/Sub-Systemen/Komponenten-Ebene aus den Sicherheitsanforderungen auf Fahrzeugebene auf Basis einer Sicherheitsargumentation.

Aufgabenstellung II: **Inkrementelles Testen von Subsystemen und Gesamtsystemen**	
• Abbildung von funktionalen Ansprüchen auf Systemelemente und Herunterbrechen auf Sub-Systeme auf Basis einer durchgehenden Sicherheitsargumentation. • Ableitung von Testanforderungen inklusive Metriken	**II.2:** Strukturierte Anforderungsdefinition an Systeme und Tests; Definition eines Testprozesses und Testvorgehens für die Absicherung von Level4/5-Systemen; Traceability, Nachvollziehbarkeit und Vergleichbarkeit von Testergebnissen über den gesamten Testprozess hinweg; Vorbereitung für die Standardisierung von Freigabetests für Level4/5-Systeme. **II.3:** Metriken und Bewertungskriterien zur Freigabe von Level4/5-Systemen.

2.1.3 Aufgabenstellung III: Nahtloses Testen über alle Testinstanzen

2.1.3.1 Ausgangssituation

Der reine Realfahrzeugversuch, wie er bei teilautomatisierten Fahrfunktionen zur Absicherung Anwendung findet, ist in seinem Umfang für diesen großen Testraum entweder nicht ausreichend oder in seinem Aufwand nicht leistbar. Die Simulation ermöglicht hier ergänzend einen skalierbaren Ansatz, um eine sehr große Anzahl von Szenarien in endlicher Zeit abtesten zu können. Zudem können z.B. konkrete Fahrsituationen bezüglich Einflussfaktoren simulativ variiert werden oder neue Kombinationen von Einflussfaktoren erzeugt werden, die so nicht in Realfahrten ermittelt wurden. Des Weiteren kann die simulative Erzeugung von Variationen real eingefahrener Fahrsituationen gezielt dafür genutzt werden, gefährliche Situationen zu erzeugen, die man mit einem Fahrzeug aus Sicherheitsgründen nicht einfahren kann.

Neben der Bewältigung eines enormen Testvolumens ist eine zentrale Herausforderung der Nachweis der fehlerfreien Funktion innerhalb dieser großen Anzahl von Tests, aber auch der Nachweis, dass die so gewonnenen Testergebnisse die Realität hinreichend gut abbilden. Hierbei ist das Zusammenspiel der Testinstanzen entscheidend. Die Nutzung der Simulation zur Prüfung hat gegenüber Realtests nicht nur den Vorteil, dass sie deutlich aufwandsärmer und zeitsparender ist, sie ist auch bezüglich der Variationsmöglichkeiten deutlich flexibler. Die zentrale Forschungsfrage von **Aufgabenstellung III** war:

Aufgabenstellung III: Nahtloses Testen über alle Testinstanzen.

Wie kann eine nahtlose Argumentationskette für den Sicherheitsnachweis aufgebaut werden in der sich Simulation und Realtest so ergänzen, dass Aufwände für Realtests minimiert und der Nutzen der Simulation für die Absicherung optimiert werden?

2.1.3.2 Ansatz von Aufgabenstellung III in VVMethoden

VVMethoden hat den Ansatz verfolgt, Simulations- und Realtests eng zu verzahnen und so auszulegen, dass sie sich durch Nutzung ihrer jeweiligen Stärken ergänzen.

Wenn die Testfallbeschreibung und die Testergebnisse der verschiedenen Testinstanzen – d.h. sowohl von Realfahrzeugtests, Einzel- oder Mehrkomponententests als auch aus Tests innerhalb

einer Simulation – nachverfolgbar und aufeinander abgestimmt sind, dann können die Stärken der jeweiligen Testinstanzen optimal genutzt werden. Auf diese Weise entstand die Möglichkeit einer umfassenden als auch effizient erzeugbaren Sicherheitsaussage. Tests in der Simulation und im Realfahrzeug mussten sich nahtlos zur Sicherheitsargumentation zusammenfügen lassen. Dazu musste der Nachweis erbracht werden, dass die Simulation die Realität hinreichend genau abbildet, so dass Teile der Tests in die Simulation verlegt werden können und im Zusammenspiel von Real und Simulationstests ein Sicherheitsnachweis möglich ist.

Ansatz III: Erzeugung einer durchgängigen, effizienten Prüfkette von Simulation bis Realfahrten, die die jeweiligen Stärken der einzelnen Testinstanzen nutzt und deren Ergebnisse effizient zu einer Gesamtsicherheitsaussage zusammengefasst werden können.

- Etablierung der Simulation als Rückgrat der Gesamttestinfrastruktur
- Erarbeitung und Darstellung der durchgängigen Testmethodik und strukturierte Anforderungsdefinition an Testinfrastukturen.
- Aufbau einer kompletten Prüfkette von Simulation über Prüfstand bis zu Realfahrten die einer Sicherheitsargumentation genügt.

Mit diesem Vorgehen hat VVMethoden ermöglicht, dass Testmittel durchgängig verwendet werden können – virtuelle und reale Testmittel wurden modular austauschbar und Tests konnten durchgängig in allen Testinstanzen durchgeführt werden. Die Ergebnisse sind (1) Sicherheitsnachweise für L4/L5-Fahrzeuge die Simulationstests und Realtests optimale kombinieren, (2) Methoden zur durchgängigen Testbeschreibung über alle Testinstanzen sowie neuartige Bewertungsmetriken und (3) der Aufbau einer durchgängigen Absicherungsplattform und die Demonstration eines durchgängigen Sicherheitsnachweises für eine exemplarische L4/L5 Fahrfunktion.

2.1.3.3 Zusammenfassung technisch/wissenschaftliches Aufgabenstellung III: Nahtloses Testen über alle Testinstanzen.

Aufgabenstellung III: **Nahtloses Testen über alle Testinstanzen.**	
Ansatz	Ergebnisse
Erzeugung einer durchgängigen, effizienten Prüfkette von Simulation bis Realfahrten, die die jeweiligen Stärken der einzelnen Testinstanzen nutzt und deren Ergebnisse effizient zu einer Gesamtsicherheitsaussage zusammengefasst werden können. • Effiziente Verifikation und Validierung durch Skalierbarkeit verschiedener Testinstanzen wie z.B. Wiederverwendbarkeit von Testeingangsdaten, Vergleich der Testergebnisse der jeweiligen Testinstanzen untereinander.	**III.1:** Sicherheitsnachweis für L4/L5-Fahrzeuge durch optimale und effiziente Verzahnung von Simulationstests und Realtests. **III.2:** Methoden zum durchgängigen Testen über alle Testinstanzen inkl. aufeinander abgestimmte Testbeschreibungen sowie zugehörige Bewertungsmetriken.

Aufgabenstellung III: **Nahtloses Testen über alle Testinstanzen.**	
• Effizientes Zusammenfügen zu einer umfassenden Sicherheitsargumentation über einheitliche Schnittstellen, Formate und Bewertungsmetriken, zugehöriger Methodenentwicklung • Aufbau einer Absicherungsplattform zur Demonstration der Umsetzbarkeit und Nachweis der Methode	**III.3:** Aufbau einer Absicherungsplattform und Demonstration eines durchgängigen Sicherheitsnachweises für eine exemplarische L4/L5-Fahrfunktion.

2.2 Voraussetzungen für das Vorhaben

Die Voraussetzungen für eine effektive, effiziente und erfolgreiche Umsetzung der Projektziele des Vorhabens VVMethoden waren hervorragend, da

- das Gros der Konsortialpartner auf umfassende Erfahrungen in der Zusammenarbeit in vorwettbewerblichen Forschungs- und Entwicklungsprojekten zurückgreifen konnte,
- viele Konsortialpartner in weiteren Forschungs- und Entwicklungsprojekten aktiv waren, innerhalb derer weitere relevante Aspekte der Verifikation und Validierung hochautomatisierter und autonomer Fahrzeuge untersucht wurden und derart der Transfer aktueller Ergebnisse - zur Projektlaufzeit - in das Vorhaben VVMethoden sichergestellt war und
- das Konsortium auf eine Vielzahl von – insbesondere auf Seiten der wissenschaftlichen Partner – verfügbaren digitalen Infrastrukturen und Datenquellen zurückgreifen konnte, auf diese aufgesetzt hat und im Rahmen des Vorhabens VVMethoden weiterausgebaut und qualifiziert hat.

Das Projekt VVMethoden konnte auf eine breite Beteiligung aller relevanten Partner aus Industrie und Wissenschaft bauen, die ihre Kompetenzen in Forschung und Umsetzung eingebracht haben. Damit wurden zum einen die Voraussetzungen für eine qualitativ hochwertige, termin- und budgetgerechte Umsetzung der Projektziele geschaffen. Zum anderen war dies der Garant dafür, dass die im Projekt VVMethoden erarbeiteten Lösungen relevant für die Industrie sind und langfristig eingesetzt werden.

Auf Seiten der *Industrie* beteiligten sich Unternehmen, die die Perspektive der OEM (Audi, BMW, Daimler, FORD, Opel, VW) und der Tier1 (BOSCH, Continental, Valeo, ZF AG) einnehmen. Darüber hinaus waren relevante Technologieprovider (AVL, dSPACE, PROSTEP, understandAI) mit eingebunden. Mit dem TÜV SÜD wurde ein Projektpartner in das Konsortium integriert, der über zentrales Know-how in der Homologation und in der regulativen Freigabe von Systemen im Fahrzeug verfügt.

Darüber hinaus waren die relevanten *Wissenschaftspartner*, die über zentrale methodische Kompetenzen für die Verifikation und Validierung automatisierter Fahrzeuge verfügen, in das Projekt eingebunden. Mit den Partnern DLR, ika, FZD, FZI, IfR, FhG und OFFIS, die während der Projeklaufzeit ein Institut des DLR wurden, konnten namhafte Wissenschaftsakteure aus dem

universitären und außeruniversitären Bereich für die Arbeit am Projekt VVMethoden gewonnen werden.

Die Wissenschaftspartner haben einen entscheidenden Teil dazu beigetragen, dass die nötige, disruptive Effizienzsteigerung der Prüf- und Instanziierungsprozesse erreicht wurde. Ihnen kamen zentrale Aufgaben im Bereich der Entwicklung der Kritikalitätsanaylsen, der Entwicklung von Sicherheitskonzepten sowie der Entwicklung von Testinfrastrukturen und Datendanken (nicht wettbewerbsdifferenzierend) zu. Damit konnte gewährleistet werden, dass der vorwettbewerbliche Ansatz von VVMethoden diskriminierungsfrei umgesetzt wurde und dass die Ergebnisse bei allen Industriepartnern zeitnah und effizient Eingang in die Wertschöpfungskette gefunden haben.

Nur im Zusammenspiel aller beteiligten Partner im Wertschöpfungsprozess konnte sichergestellt werden, dass die zu erarbeitenden Lösungen für den Einsatz in der Industrie geeignet sind. Die große Zahl an Varianten von Fahrzeugen mit unterschiedlichen Ausstattungen an Sensoren und Komponenten sowie die hohe Geschwindigkeit mit der neue Komponenten entwickelt werden, bedingt neue Konzepte für Verifikation und Validierung. Bereits für das Zusammenspiel zwischen Zulieferern verschiedener Ebenen und Fahrzeugherstellern während der Entwicklung neuer Systeme mussten daher gemeinsame Methoden und akzeptierte Systematiken gefunden werden.

Das starke Zusammenwirken der Partner wurde auch in der Projektorganisation deutlich: Industrie und Wissenschaftspartnern haben die Verantwortung und Führung des Projektes gemeinsam („Doppelspitze“) wahrgenommen (siehe auch Tabelle 1: TP-LeitungenTabelle 1).

Tabelle 1: TP-Leitungen

Teilprojekt	TP-Leitung Industrie	TP-Leitung Wissenschaft
TP1: Rahmenbedingungen und Impulsgeber	Opel	IfR
TP2: Kritikalitätsanalyse	Mercedes-Benz und ZF	DLR (ehemals OFFIS)
TP3: Sicherheitsanalyse und funktionale Architektur	BOSCH	IfR
TP4: Regelwerk System- und Testanforderungen	Mercedes-Benz	FhG
TP5: Simulationssteuerung	TÜV Süd	DLR
TP6: Datenbereitstellung	AVL	FZD
TP7: Exemplarische Testumgebung und -Anwendung	ZF AG	FZI
TP8: Datenbanken	AVL	ika
TP9: Prozess Instanziierung, kontinuierlicher Verbesserungsprozess, Anwendung und Bewertung	PROSTEP	-

2.3 Planung und Ablauf

2.3.1 Planung

VVMethoden hat als vorwettbewerbliches Verbundprojekt die nötigen Stakeholder und Kompetenzträger aus Industrie und Wissenschaft zusammengebracht, um die Projektziele effizient zu verfolgen und die entstandenen Ergebnisse nah an den Bedürfnissen der Industrie bereitzustellen. VVM ist ein Projekt der VDA Leitinitiative autonomes und vernetztes Fahren (siehe auch Kapitel 2.5.1) und als solches auch Mitglied der PEGASUS Projektfamilie zu der neben VVMethoden die Projekte PEGASUS und SetLevel gehören. Im Vorläuferprojekt PEGASUS wurden wichtige Ansätze und Ergebnisse erarbeitet auf denen VVM aufbaut, SetLevel als zeitlich überlappendes Projekt war inhaltlich direkt mit VVMethoden verbunden, dort wurden Simulationen und Simulationsmodelle entwickelt, deren Anforderungen in VVMethoden erarbeitet wurden.

2.3.1.1 Teilprojekte

Die relativ große Zahl von neun Teilprojekten spiegelt die vielfältigen Arbeitsgebiete wider, die zur Bewältigung der komplexen Aufgaben beigetragen haben. Die Teilprojekte 1 "Rahmenbedingungen und Impulsgeber" und 9 "Prozess Instanziierung, kontinuierlicher Verbesserungsprozess, Anwendung" hatten dabei projektübergreifende Sonderfunktionen und waren mit allen anderen TPs in kontinuierlichem Austausch.

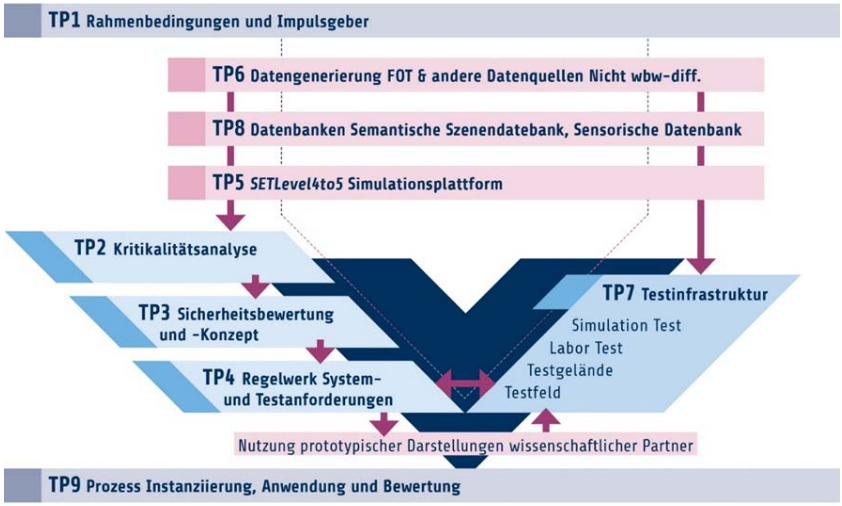


Abbildung 1: Die TPs aus VVM und deren Zusammenhang

TP1 Rahmenbedingungen und Impulsgeber fungierte als Befähigungs-TP, das zu Beginn umfassende Rahmenbedingungen sicherstellt und im weiteren Verlauf darauf achtet, dass eine gesamtheitliche Projektperspektive beibehalten wird. Die unterschiedlichen Erkenntnisstränge wurden zusammengefügt und -gehalten um ein kohärentes und nutzbares Gesamt-Projektergebnis zu erreichen. Dieser starke inhaltliche Aspekt wurde durch die in einem Projekt dieser Größe nötigen, vielfältigen administrativen Aufgaben ergänzt. Eine weitere wichtige Aufgabe von TP1 bestand in der Ergebnisverbreitung um zu gewährleisten, dass die VVM-Ergebnisse in der internationalen Fachcommunity kommuniziert wurden, diskutiert werden und letztlich Eingang in die nötigen Gremien finden.

In **TP2 Kritikalitätsanalyse** wurden, aufbauend auf den Anforderungen, Anwendungsfällen und Metriken aus TP1 die Methoden der Kritikalitätsanalyse entwickelt, die in die Sicherheitsanalysen von TP3 und in die Erstellung der Gesamtmethodik von VVMethoden (TP1) einfließen. Weiterhin

lieferte TP2 Anforderungen an Simulationsplattformen (TP5) und an die Datenerhebung aus Realfahrten (TP6) aus Sicht der Kritikalitätsanalyse.

In **TP3 Sicherheitsanalyse und funktionale Architektur** wurden aus den Kritikalitätsanalysen von TP2 Sicherheitsanalysen entwickelt aus denen wiederum Sicherheitskonzepte für TP4 abgeleitet wurden. Das beinhaltete globale und lokale Betrachtungen sowie deren Interaktion.

TP4 Regelwerk System- und Testanforderungen hat, basierend auf den in TP 3 durchgeführten Sicherheitsanalysen, den daraus entwickelten Sicherheitskonzepten und der funktionalen Systemarchitektur dann System- und Testanforderungen für die Homologation abgeleitet. Ziel war es, Methodiken zur Prüfung des Gesamtfahrzeuges über die Prüfung von Ansprüchen an Systeme/Sub-Systeme/Komponenten zu entwickeln, so dass Hersteller und Zulieferer getestete Systeme und Tests austauschen sowie Tests wiederverwenden können. Ebenso sollte die Methodik erlauben, die Testbarkeit der Sicherheit von Anfang an im Systemdesign zu berücksichtigen. TP4 widmete sich damit vornehmlich den Grundkonzepten II und III für die System- und Testanforderungen, die basierend auf einer Sicherheitsargumentation hierarchisch herunter gebrochen wurden.

TP5 Simulationssteuerung hat im Rahmen des Projektes VVMethoden die Simulationstechnologie und die Methoden zu ihrer Anwendung bereitgestellt. Dabei wurden zwei Hauptanwendungszwecke verfolgt, die Kritikalitätsanalyse im TP2 und die Absicherung von automatisierten Fahrzeugen und deren Komponenten (Sensorik, Fahrfunktionen etc.) im TP7. In der Kritikalitätsanalyse wurde sie zur Ableitung und Analyse relevanter Szenarien genutzt, an denen die Kritikalitätsphänomene studiert, präzisiert und bewertet werden können. Bei der Absicherung diente sie dem umfassenden Testen von Systemen oder Komponenten von Systemen.

Im **TP6 Datenbereitstellung** wurden Messdaten generiert, aufbereitet und im Projekt zur Verfügung gestellt. Die Daten wurden dabei durch wissenschaftliche Partner mit bestehenden Fahrzeugen sowie durch AVL mit einem für das Projekt aufgebauten Versuchsträger erzeugt. Zusätzlich wurden in der Anwendungsplattform Intelligente Mobilität (AIM) Daten einer Braunschweiger Kreuzung erhoben. Weitere Daten lieferte das Karlsruher Testfeld automatisiertes Fahren (TAF) sowie die mobile Messtechnik des FhG-IVI.

In **TP7 Testvorgehen** wurden die Testanforderungen aus TP4, die Simulationswerkzeuge aus TP5, die in TP9 ermittelten wettbewerbsdifferenzierenden Anforderungen sowie Anforderungen und Vorarbeiten aus Forschungsprojekten wie bspw. PEGASUS verwendet, um daraus ein Testvorgehen für die Absicherung von L4/L5-Systemen zu entwickeln. Dies hat insbesondere das identifizierte technisch/wissenschaftliche Arbeitsziel III „Nahtloses Testen über alle Testinstanzen“ adressiert.

Kernziel von **TP8 Datenbanken** war die Verarbeitung der im Projekt benötigten und erzeugten Daten in einer zentralen Datenbank. TP8 hat somit die technische Basis für die Erzeugung einer durchgängigen, effizienten Prüfkette von Simulation bis Realität zur Verfügung gestellt.

TP9 Prozess Instanziierung, kontinuierlicher Verbesserungsprozess, Anwendung hatte zu Aufgabe der Anforderungen der Industriepartner zu sammeln und zu bündeln, insbesondere die der Projektpartner, die nicht an den entsprechenden TPs 2-8 beteiligt waren. hatte zu Aufgabe der Anforderungen der Industriepartner zu sammeln und zu bündeln, insbesondere die der Projektpartner, die nicht an den entsprechenden TPs 2-8 beteiligt waren. Das Teilprojekt 9 leistet

zusätzlich einen Beitrag zur Qualitätssicherung und zur Erhöhung der Marktakzeptanz der Ergebnisse jedes Teilprojekts. Die Brückenfunktion und die transparente Nachverfolgbarkeit („Traceability“) der Ergebnisse werden durch das Baselining-Tool aus Teilprojekt 1 sowie durch die SysML-basierte Dokumentation der Gesamtmethode unterstützt. Dadurch wird zum einen das Projektmanagement erleichtert und zum anderen die sichere Nachvollziehbarkeit der Ergebnisse gewährleistet. In diesem Kontext koordiniert das Teilprojekt 9 die kontinuierliche Weiterentwicklung und Verbesserung des Modells sowie der Implementierung. Zudem erfolgt eine Harmonisierung der innerhalb der VVM-Gesamtmethode erstellten Prozesse und Artefakte in enger Zusammenarbeit und Abstimmung mit den Projektpartnern. Dies unterstützt die spätere industrielle Anwendbarkeit der Ergebnisse.

2.3.1.2 Projektphasen

Die Arbeiten in VVMethoden wurden in drei Phasen konzipiert, wie in Abbildung XXX dargestellt:

- **Phase 1 – Ansatzphase** – Aufstellen der zentralen Ansätze auf Basis der Stand der Technik und im Wesentlichen auf Basis bestehender Daten.
- **Phase 2 – Vertiefungsphase** – Ausarbeitung und Konkretisierung der Ansätze auf Basis nicht automatisierter Fahrten und Einbeziehung der Simulation.
- **Phase 3 – Komplettierungsphase –** industriegerechte, effiziente Verknüpfung der Ansätze, Quercheck. Finale Einbeziehung von Automationsrisiken über Datenanreicherung auf Basis von Fahrten mit SAE-Level 4/5 Fahrfunktionen.

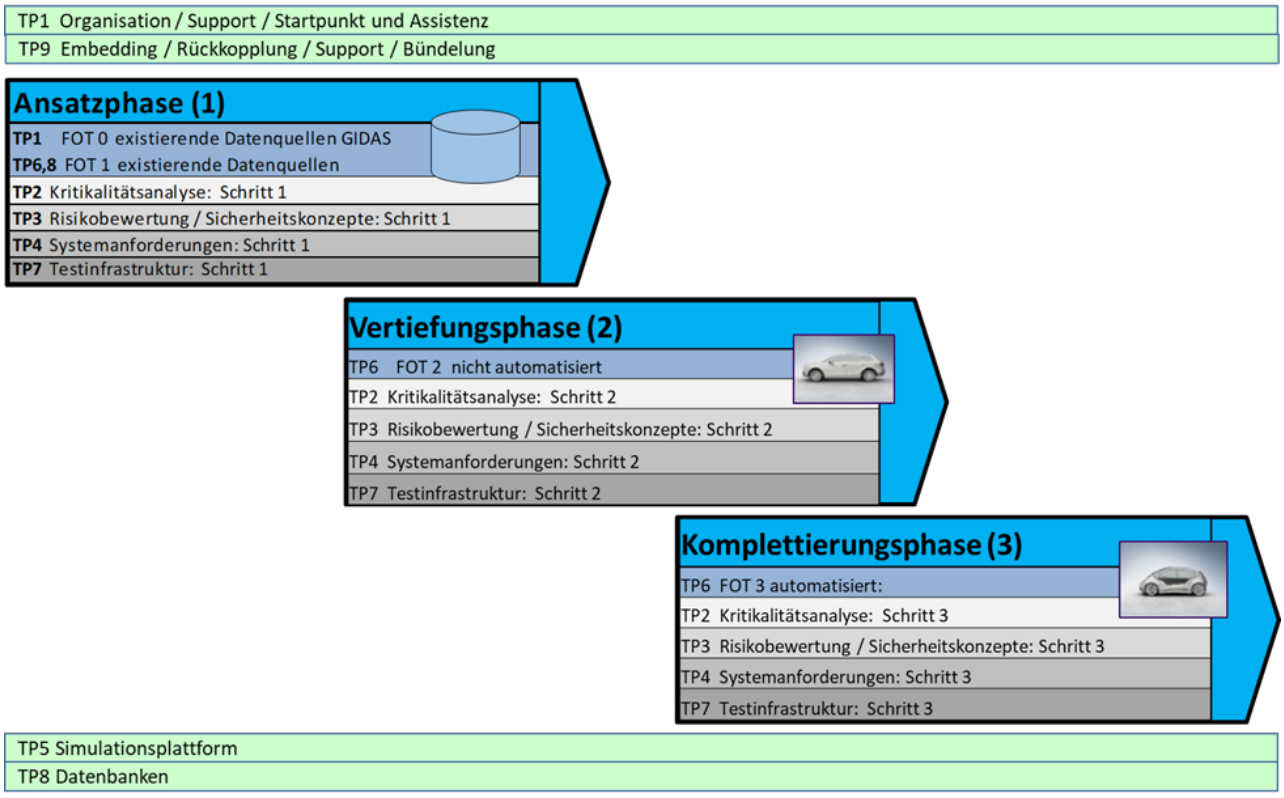


Abbildung 2: Die drei Arbeitsphasen in VVMethoden.

Durch diesen iterativen Ansatz wurde zum einen gewährleistet, dass neue Ansätze und Erkenntnisse die außerhalb des Projektes entstanden sind auch während der Projektlaufzeit

aufgenommen werden konnten. Zum anderen konnten so schon frühe Versionen der Ergebnisse ausgeleitet werden, um sie bei den beteiligten Herstellern und Zulieferern zu erproben oder in externen Kreisen diskutiert und reflektiert werden.

2.3.2 Ablauf

2.3.2.1 Covid-19 Pandemie

Die Projektlaufzeit war initial von 07/2019 bis 06/2023 geplant. Damit fiel der Beginn der Covid-19-Pandemie in das dritte Projektquartal. Diese hatte für VVM verschiedene Auswirkungen:

- Die kurzfristige Umstellung auf vollständiges Homeoffice hat zu Ausfällen, Nichtverfügbarkeiten und reduzierter Effizienz geführt, welche die Projektarbeit merklich verzögert haben.
- Die physischen Treffen wurden eingestellt und waren erst sehr spät wieder in der geplanten Breite möglich. Dies betraf nicht nur die klassischen Arbeitsmeetings und Konsortialtreffen, die einen großen Teil der Projektlaufzeit als Videokonferenzen abgehalten werden mussten, oder die Halbzeitpräsentation bei der nur ein Redner-Rumpfteam zusammenkam während alle Zuschauer remote teilnehmen mussten.
    - Zur tieferen Reflektion der Absätze und um früh und mehrfach die Projektergebnisse mit der Fachcommunity zu diskutieren waren am Ende jeder Projektphase "Offene Treffen zur Ergebnisverbreitung" vorgesehen, die in dieser Form nicht stattfinden konnten.
    - Außerdem war in TP9 verankert die Industriepartner aufzusuchen und deren Feedback zu (1) Anforderungsmanagement, (2) Harmonisierung Werkzeugschnittstellen und Dateiformate und (3) Instanziierung der Verifikations- und Validierungsmethodik einzuholen, um es aufzubereiten und in das Projekt zurückzuspielen. Auch das musste Remote durchgeführt werden.

Um die ambitionierten Projektziele auch unter diesen Umständen zu erreichen wurde eine kostenneutrale Projektverlängerung von sechs Monaten beantragt, die vom Projektträger bewilligt wurde.

2.3.2.2 Rückzug Visteon

Im ersten Halbjahr 2020 erklärte der Konsortialpartner Visteon seinen Rückzug aus dem Projekt. Der Großteil der von Visteon zu erbringenden Arbeitsinhalte war zu diesem Zeitpunkt noch nicht erbracht. Die Konsortialführung hat daraufhin große Anstrengungen unternommen für alle diese Beiträge Konsortialpartner zu finden, die sie übernehmen könnten. Dies gelang letztendlich und wurde in einer überarbeiteten Vorhabenbeschreibung dokumentiert. Nachdem der Projektträger seine Zustimmung zur veränderten Arbeitsteilung und daran gekoppelt zur ebenfalls modifizierten Budgetverteilung gegeben hatte, wurde der Rückzug zum 30.06.2020 in einer Austrittsvereinbarung zum Konsortialvertrag juristisch festgeschrieben.

2.3.2.3 Erweiterung Datenbankkonzept

Ebenfalls im ersten Halbjahr 2020 wurde klar, dass das in TP8 verankerte Datenbankkonzept erweitert werden musste. Geplant war in der Vorhabenbeschreibung eine zweigeteilte, zentrale Datenbank, die einerseits Szenarien und andererseits Sensordaten und gegebenenfalls deren

Annotierungen enthalten sollte. Mit diesem Ansatz hätte die für alle Projektpartner zugängliche Sensordatenbank aber bis zur Anonymisierung auch personenbezogene Daten enthalten. Die durch die DSGVO deswegen nötigen rechtlichen Absicherungen hätten allerdings beträchtliche juristische Abstimmungen mit unabsehbaren zeitlichen Konsequenzen nach sich gezogen. Dankenswerterweise hat der in TP8 federführende Industriepartner AVL angeboten eine zusätzliche Rohdatenbank mit stark eingeschränktem Zugriff aufzubauen ("Safety Cage") um diese Problem zu umgehen.
Außerdem wurde der starke Bedarf für einen vielseitigeren Zugriff auf die Szenariendatenbank sowie deren Erweiterung zu einer Entwicklungsdatenbank erkannt, mit der andere TPs partnerübergreifende und iterative Auswertungen zur Identifikation und Plausibilisierung von Kritikalitätsphänomenen und Wirkzusammenhängen durchführen können. Hier konnte das ika mit dem ITCenter der RWTH eine Lösung anbieten und mit der dort betriebenen Forschungsdatenbank CoScInE den benötigten Service bereitstellen.

2.4 Stand der Wissenschaft und Technik

Dem Stand der Wissenschaft und Technik zu Beginn des Förderprojektes V&V Methoden lagen grundsätzlich die gesetzlichen Vorgaben (Legal Frameworks) als auch etablierte Sicherheitsstandards der Entwicklung, z.B. in der ISO oder UN-ECE, zu Grunde. Auf Basis dieser Randbedingungen entwickeln alle Automobilhersteller und Zulieferer ihre Fahrerassistenzfunktionen für ihre Fahrzeugmodelle, d.h. Funktionen mit einem Automatisierungsgrad < SAE Level 3. Bei dieser Teilautomatisierung hat der Fahrer die Verantwortung, die Fahrfunktion ständig zu überwachen und muss bei Fehlverhalten ggf. übernehmen. Entsprechend sind diese Standards ausgelegt. Für den Betrieb von SAE Level 3 Funktionen sind seit dem Förderprojekt PEGASUS einige Regularien dazu gekommen, die es nun ermöglich automatisierte Fahrfunktionen mit SAE Level 3 auf der Straße zu testen oder als Serienprodukt zu entwickeln.

2.4.1 Legal Frameworks

Das älteste, aber immer noch gültige Legal Framework ist das Wiener Übereinkommen von 1968, welches die Regeln für den Straßenverkehr und die Verkehrssicherheit fest. Es besagt, dass der Fahrer jederzeit die Kontrolle über sein Fahrzeug haben muss (Vereinte Nationen, 1969). 2014 hat die UN-ECE diese Regelung dahingehend erweitert, dass automatisierte Systeme grundsätzlich erlaubt sind, wenn diese weiterhin einen Fahrer haben, der bereit ist, die Fahrfunktion zu überwachen und ggf. zu übernehmen und der hierzu auch technisch in die Lage versetzt wird. Infolgedessen hatten zu Beginn von VVM verschiedene internationale Organisationen und Regierungen begonnen, neue Richtlinien und Regelungen für das automatisierte Fahren zu entwickeln, die das Wiener Übereinkommen ergänzen oder aktualisieren. Ein Beispiel hierfür war zu Projektbeginn die Arbeit der Vereinten Nationen (UN) und ihrer Wirtschaftskommission für Europa (UNECE), die die Entwicklung des "Übereinkommens der Vereinten Nationen über Straßenverkehrsregeln" vorantrieben und auch aktuell noch vorantreiben.

Dieses neue Übereinkommen soll die Herausforderungen des automatisierten Fahrens berücksichtigen und einen internationalen Rahmen für den Betrieb und die Zulassung automatisierter Fahrzeuge schaffen. Es soll auch die Rechte und Pflichten von Fahrern, Herstellern und Regierungen in Bezug auf automatisierte Fahrfunktionen klären. Obwohl das Wiener Übereinkommen von 1968 in einigen seiner Aspekte weiterhin relevant sein kann, wird es zunehmend durch spezifischere Regelungen und Standards für das automatisierte Fahren ergänzt oder ersetzt.

Auf Europa bezogen veröffentlichte die Europäische Union im August 2020 die ALKS-Regulierung. Dieses regelt die Verwendung von Automated Lane Keeping Systems (ALKS). Im Folgenden werden die wichtigsten Inhalte und der Geltungsbereich der Verordnung zusammengefasst:

- Definition von ALKS: Die Verordnung definiert Automated Lane Keeping Systems (ALKS) als Systeme, die für kurze Zeit die Längsführung und Querführung eines Fahrzeugs auf Autobahnen oder autobahnähnlichen Straßen übernehmen können, ohne dass der Fahrer ständig die Fahrzeugführung überwachen muss.
- Gültigkeitsbereich: Die Verordnung gilt für alle Mitgliedsstaaten der Europäischen Union und betrifft Fahrzeuge, die mit ALKS ausgestattet sind oder mit ALKS nachgerüstet werden.
- Sicherheitsanforderungen: Die Verordnung legt strenge Sicherheitsanforderungen fest, die ALKS erfüllen müssen. Dazu gehören unter anderem die Zuverlässigkeit der Sensoren und Aktuatoren, die Funktionsfähigkeit des Systems unter verschiedenen Bedingungen (z. B. Wetter, Verkehrsdichte) sowie die Einhaltung der Verkehrsregeln und die Fähigkeit, in Notsituationen sicher zu reagieren.
- Fahrerüberwachung: Obwohl ALKS die Fahrzeugführung übernehmen können, müssen die Fahrer weiterhin in der Lage sein, das System zu überwachen und bei Bedarf die Kontrolle zu übernehmen. Die Verordnung schreibt vor, dass ALKS das Verhalten des Fahrers überwachen und ihn auffordern müssen, die Kontrolle zu übernehmen, wenn dies erforderlich ist.
- Genehmigungsverfahren: Hersteller von ALKS müssen die Systeme vor ihrer Verwendung auf dem Markt genehmigen lassen. Dies umfasst umfassende Tests und Prüfungen, um sicherzustellen, dass das System den Anforderungen entspricht und sicher ist.
- Haftung: Die Verordnung legt auch Regeln zur Haftung fest, insbesondere im Falle von Unfällen oder Schäden, die durch ALKS verursacht werden. Die Haftung kann sowohl beim Hersteller des Systems als auch beim Fahrer liegen, je nach den Umständen des Vorfalls.

Außerhalb Europas wurden ähnliche Regularien und Richtlinien für automatisierte Fahrfunktionen veröffentlicht, die je nach Land oder Region variieren. Einige Beispiele sind:

- USA: Die National Highway Traffic Safety Administration (NHTSA) in den USA hat verschiedene Richtlinien und Regelungen für automatisierte Fahrzeuge, einschließlich solcher, die sich auf autonome Fahrfunktionen wie Spurhalteassistenten oder Adaptive Cruise Control beziehen. Vor Projektbeginn lag das Dokument “Automated Driving Systems (ADS) 2.0” des Departement of Transportation vor. Dieses umfasste Richtlinien für die Entwicklung und den sicheren Einsatz von automatisierten Fahrsystemen in den USA.
- China: China hat ähnliche Vorschriften und Standards für automatisierte Fahrfunktionen wie die Europäische Union. Die chinesische Regierung hat Richtlinien veröffentlicht, die die Entwicklung und den Einsatz autonomer Fahrzeuge regeln, um die Sicherheit auf den Straßen zu gewährleisten. Zu Projektbeginn lag das Dokument „China’s Raod Test Regulation for Intelligent Connected Vehicles“ vor.

2.4.2 Safety Standards

Für die Absicherung von Funktionen und Systemen bei OEMs und Tier1s gibt es verschiedene Sicherheitsstandards und Normen. Diese bildeten zum einen die Grundlage für die Arbeiten an einem Sicherheitsnachweis für automatisierte Fahrfunktionen in VVM, stießen zum anderen aber auch an grundsätzliche konzeptionelle Grenzen. Im Folgenden sind die wesentlichen Sicherheitsstandards genannt, die in der Entwicklung von Fahrerassistenzsystemen und auch automatisierten Fahrfunktionen in der Industrie ihre Anwendung finden und in VVM berücksichtigt wurden:

1. ISO 26262: Road vehicles – Functional safety: Veröffentlicht im November 2011. Dieser Standard legt Anforderungen an die funktionale Sicherheit von elektrischen und elektronischen Systemen in Kraftfahrzeugen fest, einschließlich automatisierter Fahrsysteme ohne speziell auf diese neuen Systeme einzugehen.
2. ISO/PAS 21448: Road vehicles – Safety of the intended functionality (SOTIF): Veröffentlicht im November 2019. Dieser Standard behandelt potenzielle Missverständnisse oder Unfälle aufgrund von Sicherheitslücken bei der "beabsichtigten Funktionalität" automatisierter Fahrsysteme, insbesondere solcher, die nicht unter die funktionale Sicherheit nach ISO 26262 fallen.
3. ISO/SAE 21434: Road Vehicles – Cybersecurity engineering: Veröffentlicht im Juli 2021. Dieser Standard legt Anforderungen an das Cybersecurity-Engineering für automatisierte Fahrsysteme fest, um Risiken im Zusammenhang mit Cyberangriffen zu identifizieren, zu bewerten und zu behandeln.
4. SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles: Erstmals veröffentlicht im September 2014. Klassifiziert automatisierte Fahrfunktionen in sechs Stufen von Level 0 (keine Automatisierung) bis Level 5 (vollständige Automatisierung) und liefert Definitionen für Begriffe im Zusammenhang mit automatisierten Fahrsystemen.
5. UNECE Regulierung Nr. 157: Automatisierte Spurhaltefunktionen (ALKS): Veröffentlicht im Juli 2020. Regelt die Verwendung von Automated Lane Keeping Systems (ALKS) in Fahrzeugen und legt Sicherheitsanforderungen sowie Verfahren für die Typgenehmigung fest.

Abbildung 3 gibt einen möglichst vollständigen, größeren Überblick über die zu Projektbeginn laufenden Standardisierungsaktivitäten bzgl. der Absicherung des automatisierten Fahrens im internationalen Kontext und bewertet diese bzgl. ihrer Relevanz für die VVM Inhalte.

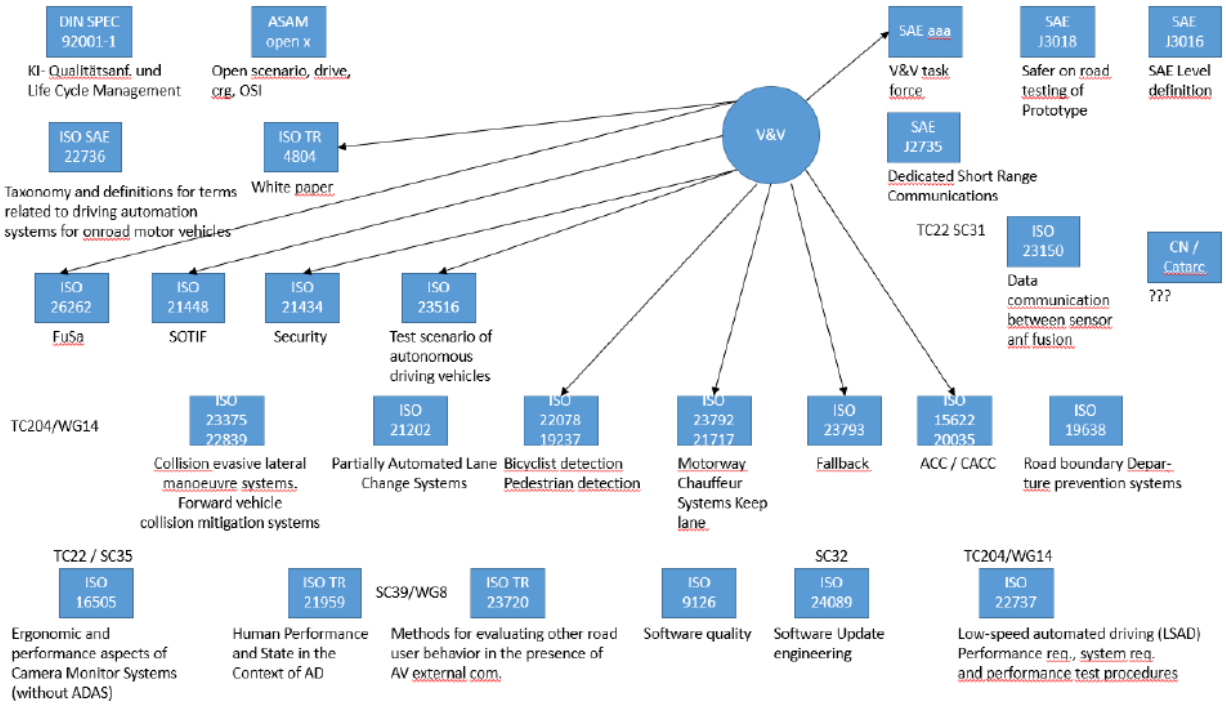


Abbildung 3: Übersicht der Standardisierungsaktivitäten zum automatisierten Fahren.

2.4.3 Safety Reports

Die National Highway Traffic Safety Administration (NHTSA) in den USA fordert von Herstellern von automatisierten Fahrfunktionen Safety Reports ein. Diese Anforderung ist Teil der Richtlinien, die von der NHTSA für die Entwicklung und den Betrieb automatisierter Fahrsysteme festgelegt wurden.

Der Safety Report soll eine detaillierte Beschreibung des automatisierten Fahrsystems sowie seiner Sicherheitsstrategie und -maßnahmen enthalten. Dazu gehören unter anderem Informationen über die Funktionsweise des Systems, das Sicherheitsdesign, die Prüfverfahren, Unfallstatistiken, Pläne für die Schulung von Fahrern oder Bedienern und vieles mehr. Durch diese Safety Reports will die NHTSA sicherstellen, dass die automatisierten Fahrsysteme sicher entwickelt, getestet und betrieben werden, bevor sie auf öffentlichen Straßen eingesetzt werden dürfen. In diesem Sinne legen diese Reports den Stand der Technik mit fest und helfen dabei Best-Practise Ansätze zu finden. In den USA wird von folgenden Firmen regelmäßig ein Safety Report für die jeweilige automatisierte Fahrfunktion veröffentlicht:

1. Waymo (Alphabet Inc./Google): Waymo veröffentlicht regelmäßig Safety Reports, in denen sie ihre Ansätze zur Sicherheit von autonomen Fahrzeugen erläutern. Diese Berichte enthalten Informationen zu Sicherheitsmaßnahmen, Unfallstatistiken und Prüfverfahren. Die Berichte von Waymo geben Einblick in die Entwicklungs- und Testprozesse ihrer autonomen Fahrsysteme sowie in ihre Bemühungen um Transparenz und Sicherheit.

2. GM Cruise: GM Cruise, die Tochtergesellschaft von General Motors für autonome Fahrzeuge, hat ebenfalls Sicherheitsberichte veröffentlicht, die ihre Ansätze zur Sicherheit und Prüfung autonomer Fahrsysteme beschreiben. Diese Berichte bieten Einblicke in die Entwicklungs- und

Testprozesse von GM Cruise sowie in ihre Bemühungen, die Sicherheit autonomer Fahrzeuge zu gewährleisten.

Zusammenfassend lässt sich sagen, dass zu Projektbeginn nur die ersten Schritte im Bereich Regulatorik sowie Standards und Normen für die Entwicklung, Absicherung und Zulassung automatisierter Fahrfunktionen gegangen wurde und diese Prozesse während der Laufzeit von VVM weiter vorangeschritten sind. Sie definieren neben den Safety Reports und Projektergebnissen wie die aus PEGASUS den Stand der Technik für die Absicherung automatisierter Fahrfunktionen und sind somit die Absprungbasis für VVM.

2.4.4 Stand der Technik im Bezug zu den Lösungsansätzen

Im Projekt wurde eine Methodik entwickelt, welche die in Abbildung 4 dargestellten Testarten zu einem durchgängigen Testkonzept verzahnt. In den folgenden Unterkapiteln wird der Stand der Wissenschaft und Technik für diese einzelnen Ebenen beschrieben und die daraus resultierenden Herausforderungen sowie der in VVMethoden gewählte Ansatz.

Die in Kapitel 2.1 beschriebenen technisch/wissenschaftlichen Aufgabenstellungen und Ansätze haben auf Technikbereichen aufgebaut, die nach dem Stand der Technik als Eckpfeiler in der Automobilbranche galten. Abbildung 4 den Zusammenhang der Testarten dar, zeigt auf welche Technikbereiche maßgeblich vorangetrieben wurden und ordnet diese entsprechenden Unterkapitel von Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** zu.

- **Methodik zur Ableitung von System- und Testanforderungen** – Bestandteil Ansatz II
- **Testprozess** – Bestandteil von Ansatz II / III
- **Model/SW-Testing (MiL/SiL)** – Bestandteil von Ansatz III
- **Gerätetest (HiL)** – Bestandteil von Ansatz III
- **Testen im Fahrzeug** – Bestandteil von Ansatz III

Im Folgenden wird auf die Technikbereiche näher eingegangen. Um den Zusammenhang der Technikbereiche mit den Testmöglichkeiten und der Bearbeitung im Projekt bereits hier klar zu machen,

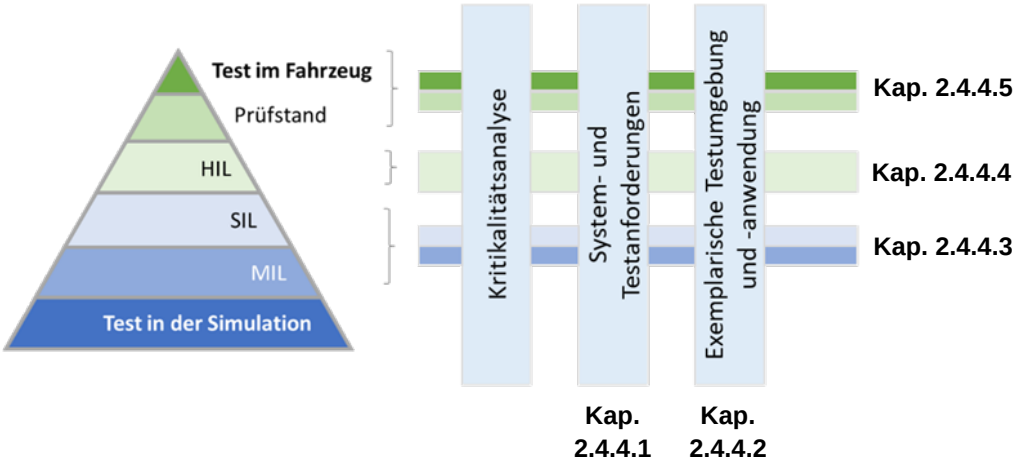


Abbildung 4: Stand der Technik, Beziehung zu Teilprojekten, Testarten und Unterkapiteln.

Die folgenden Kapitel beschreiben den Stand der Technik zu Beginn des Projektes.

2.4.4.1 Methodik zur Ableitung von System- und Testanforderungen – Bestandteil Ansatz II

L4/L5-Systeme agieren per Konstruktion selbständig („intelligent“) in Situationen, die bei der Entwicklung der Systeme nicht explizit berücksichtigt wurden. Ihre Verhaltensgrenzen waren dabei nicht genau bekannt und somit fehlte die Grundlage, um über Konsequenzen von Fehlverhalten, beziehungsweise über Abweichungen von einem als sicher angenommenen spezifizierten Verhalten nachzudenken und diesbezüglich konkrete Sicherheitsziele abzuleiten. Viele Arbeiten in der Safety-Forschungsgemeinde haben sich mit dieser Problematik beschäftigt. Alle Lösungen hatten gemeinsam, dass sie versuchten, das Risiko bezüglich ganz allgemeiner Unfallarten zur Laufzeit zu bestimmen und zu kontrollieren, wobei ein dynamisches Risikomanagement anwendungsdomänenübergreifend im Kontext von Avionik [3], Robotik [4], [5], [6], und Automotive [7] vorgeschlagen wurde. Dieses Risikomanagement muss dabei auch in den System- und Testanforderungen berücksichtigt werden.

Die Normvorgaben der ISO 26262 [8] zur Ermittlung und Ableitung von Auslegungsspezifikationen, die wiederum in Testspezifikationen überführt werden müssen, gilt prinzipiell und ist vom Grundsatz her auch für das autonome Fahren zutreffend. Auch die darin vorgesehene Einstufung diverser Verifikationsmethoden ist vom Prinzip her relevant. Doch umfasste der gedanklich-konzeptionelle Hintergrund der dort definierten Vorgehensweisen und Maßnahmen nicht das Problem eines mit seinem Umfeld autonom interagierenden Fahrzeugs, das die potentiell gefahrbringende aktive Funktion in nahezu allen erdenklichen Situationen eigenverantwortlich aktivieren und in gefahrloser Weise nutzen soll. So stellt sich die Frage, welche Methodik zur Testfallableitung und Testspezifikation für diese Systemklasse geeignet ist und ggf. welche Aktivitäten und Betrachtungsweisen ergänzend anzuwenden sind. Dies hat eine Reihe von Fragestellungen bezüglich der Herangehensweise zur Erfüllung der Normanforderungen aufgeworfen.

Die Normung zur funktionalen Sicherheit und die darauf bezogene praktische Umsetzung bezogen sich in Ihrem damaligen Stand der Technik darauf, dass ein elektrisches bzw. elektronisches System (E/E-System) im Fahrzeug mit gefährdungsrelevanter Funktionalität der Autorisierung und Verantwortung eines Fahrers unterliegt. Dessen Verantwortung wurde der angemessene Fahrzeugbetrieb und auch die Möglichkeit einer Reaktion auf besondere Situationen oder Ereignisse bzw. auf Fehler des Systems soweit möglich mildernd oder verhindernd zugeschrieben. In L4/L5-Fahrzeugen ist der „Fahrer“ selbst ein E/E-System, das der Nachweisführung für funktionale Sicherheit unterliegt. Die Natur des Funktionskonzepts „autonomes Fahrzeug“ hat damit nicht nur den nach ISO 26262 abzusichernden Funktionsumfang erheblich erweitert, sondern hat grundsätzlich neue funktionale Aspekte hinzugefügt. Deren Absicherung durch systematische Testfallableitung, Testspezifikation und -umsetzung war bisher in der Praxis und der zugrundeliegenden Normung nicht thematisiert.

2.4.4.2 Testprozess – Bestandteil Ansatz II / III

Als grundlegendes Vorgehensmodell für die Produktentwicklung in der Automobilindustrie war das in Abbildung 5 dargestellte V-Modell etabliert [9]. Das V-Modell beschreibt ein strukturiertes und sequentielles Vorgehen in der Entwicklung mit definierten Entwicklungsphasen [10].

Der linke absteigende Ast beschreibt Top-Down-orientierte Dekompositionsphasen in der Systementwicklung zur Spezifikation und Realisierung des Systems. Entsprechende Aktivitäten im

Bereich Verifikation und Validierung sind zugehörig gegenüber als Bottom-Up-orientierte Integrations- und Prüfphasen eingeordnet.

Die Aktivitäten im rechten Schenkel des V-Modells prüfen entsprechend ihrer Stufe die Umsetzung der im linken Schenkel erarbeiteten Spezifikationen und Implementierungen. Automotive SPICE [11] ist als Prozessreferenzmodell an das Vorgehen im V-Modell angelehnt und dient als Rahmenwerk für produktbezogene Entwicklungs- und Managementprozesse im Bereich der Elektrik/Elektronik für die Automobilindustrie. Konkrete Tätigkeiten und Arbeitsergebnisse für die verschiedenen Entwicklungs- und Testschritte sind definiert.

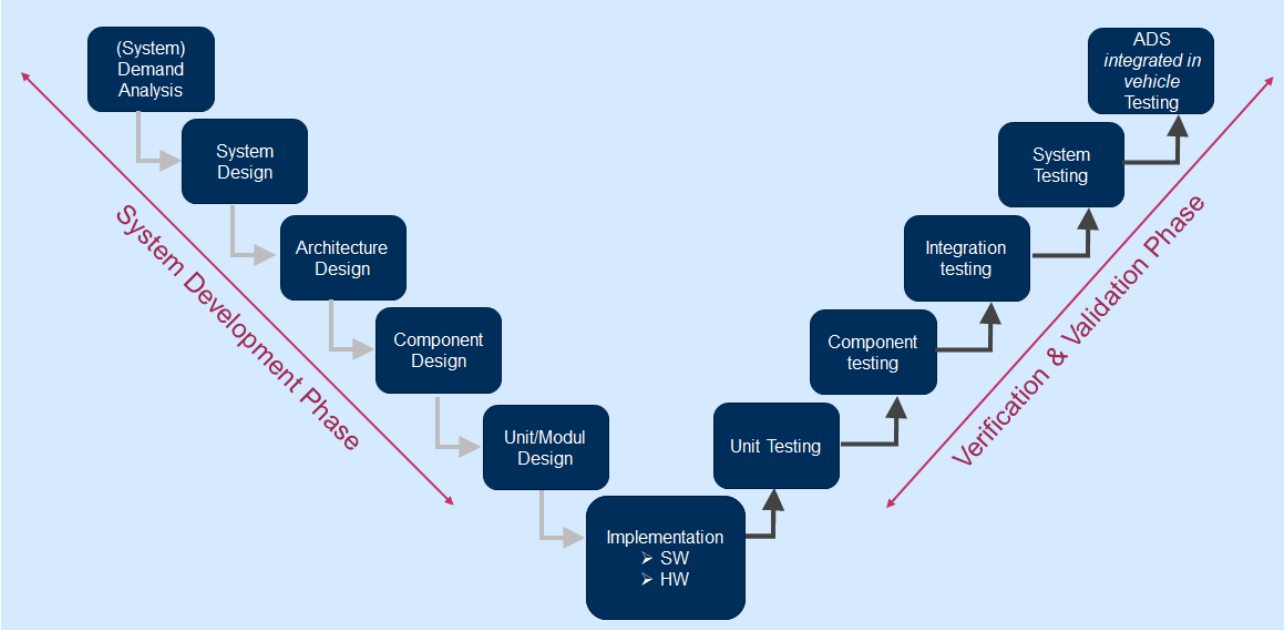


Abbildung 5: V-Modell (Prozessmodell) nach VDI-Entwicklungsmethodik für mechatronische Systeme

Der Test von Regelungssystemen erfordert einen geschlossenen Wirkungsweg um die Interaktion des Systems mit seiner Umwelt zu ermöglichen. Dieser Ansatz einer simulativen Absicherung wird auch als X-in-the-Loop (XiL) Methode bezeichnet [12]. Der Begriff „in-the-Loop“ impliziert dabei einen bidirektionalen Informationsfluss zwischen Testobjekt und Simulationsumgebung. Für die simulationsgestützte Entwicklung von Closed-Loop Systemen existieren für alle Stufen entlang des Entwicklungsprozesses spezialisierte Methoden.

Die drei gängigen Abstraktionsebenen sind Model-in-the-Loop (MiL), Software-in-the-Loop (SiL) sowie Hardware-in-the-Loop (HiL) [13], [14].

- Model-in-the-Loop (MIL) definiert den Einsatz einer Simulationsumgebung zur Generierung der Stimuli für die Entwicklung und den Test spezifizierter Funktionsmodelle (Modelle zur Abbildung des Fahrzeugsystems und seiner Umgebung) während des System- und Softwareentwurfs. Ziel der Analysen und Tests auf MiL-Ebene ist die Verifizierung des Entwurfs der logischen Systemarchitektur und der eingesetzten Algorithmen [15].
- Software-in-the-Loop (SIL) definiert den Einsatz einer Simulationsumgebung für die Ausführung und den Test von Seriencode auf Ebene der Software Systemarchitektur. Die implementierte Softwarekomponente wird dabei in die Basissoftware integriert auf einer virtualisierten Laufzeitumgebung betrieben [16]. Ziel der Tests auf SiL-Ebene ist der

Nachweis der korrekten Funktionserbringung der Softwarekomponente im Kontext des Gesamtsystems und der Systemumgebung.

- Hardware-in-the-Loop (HiL) definiert den Einsatz einer Simulationsumgebung für die Ausführung und den Test der in die Zielhardware integrierten Softwarekomponenten unter Verwendung der technischen Systemschnittstellen. Auf HiL-Ebene wird zwischen Komponenten-, Cluster- und Integrationstests unterschieden [17]. Gerätetests (Komponenten-HiL) definiert der Prüfung der gesamten Komponente, nachdem die Software in das Steuergerät integriert wurde. Hier wird ausschließlich auf die Schnittstellen des späteren Einsatzes zugegriffen, es handelt sich also um ein charakteristisches Blackbox-Verfahren. Hier wird sowohl die Widerstandsfähigkeit gegenüber Umwelteinflüssen als auch das Zusammenspiel der Hardware und Software intensiv getestet. Auch Timing-Aspekte spielen eine essentielle Rolle.

Beim Geräteverbundtest bzw. Systemverbund-Test (Cluster-HiL) wird das Zusammenspiel einzelner Subsysteme verifiziert. Fokus dieser Prüfung ist die Stabilität der Kommunikationsbusse und die Verträglichkeit der verschiedenen Steuergeräte unterschiedlicher Zulieferer im gemeinsamen elektrischen Versorgungsnetz. Zudem dient dies der Verifikation eines zusammenhängenden und verteilten Subsystems (bspw. Systemverbund Fahrerassistenz) [18]. Der Gesamtfahrzeugprüfplatz (Fahrzeug-HiL) verifiziert das Zusammenspiel aller im Fahrzeug enthaltenen E/E Systeme [19].

Um das ganze Fahrzeug auf Systemebene zu testen, werden klassischerweise in großem Umfang reale Versuchsfahrten angewendet. Diese können im ganzen Entwicklungsprozess im Rahmen von ersten Prototypen (Rapid Prototyping), Erprobungsträgern und Dauerläufern durchgeführt werden [20]. Zum Ende der Entwicklung hin sind diese insbesondere für eine Validierung der Systeme im Realbetrieb relevant. Für den Abnahmetest und die Zulassung des Fahrzeugs wird hierbei eine hohe Zahl an Testkilometern in Realfahrten benötigt. Diese werden beispielsweise bei Winter- und Sommererprobungen sowie bei länderspezifischen Erprobungen gesammelt. Dabei sind die Prüfbedingungen wie das Wetter und andere äußere Einflüsse genau definiert. Durch die hohe Zahl an benötigten Testkilometern, die hohen Kosten der Bereitstellung und Nutzung von Testfahrzeugen sowie die Anforderungen an gewisse, nicht beeinflussbare äußere Umstände ist die Zulassung durch Realfahrten ein sehr aufwändiges und kostenintensives Vorgehen.

Bei diesem klassischen Ansatz werden die durchzuführenden Testfälle in den unterschiedlichen Stufen werden im Rahmen von Testspezifikationen definiert und festgelegt. Hierbei sind die Tests systematisch aufgebaut und folgen einem stringenten Vorgehen. Basierend auf definierten Vorbedingungen werden einzelne Testschritte bspw. als Events festgelegt. Am Ende des Testschrittes werden die beschriebenen erwarteten Ergebnisse mit den Ergebnissen des Tests verglichen. Eine Aussage, ob der Test bestanden wurde erfolgt über entsprechende Testauswertungen, bspw. binäre Entscheidungen (PASS/FAIL). Die Definition der einzelnen Testschritte sowie die Überprüfung des Testfalls erfolgen zumeist über dezidierte Signale bzw. Signalverläufe, die Spezifikation der Testfälle anhand von Anforderungen an das System Somit sind die Tests zumeist synthetisch und basieren stark auf der Expertise des Testingenieurs [21].

Im Rahmen dieser Fahrzeugtests werden vom Testfahrer Erprobungskataloge abgeprüft. Diese stellen zumeist basierend auf Erfahrungswissen, verschiedene Manöver bzw. Testfälle dar. Dem Testfahrer werden basierend auf einem Anfangszustand des Fahrzeugs verschiedene Manöver (analog zu Testschritten) vorgeschrieben. Zudem sind die erwarteten Ergebnisse festgehalten-

[22]. Zum Teil werden subjektive Bewertungen z.B. durch Testfahrer herangezogen, im Gegengewicht zur erhöhten Subjektivität steht eine hohe Realitätsnähe durch das Fahrzeug und die Umwelt.

Die Testabdeckung ermöglicht eine Abschätzung des Testumfangs und unterstützt die Bestimmung des Abschlusses eines Testumfangs [23]. Sie kann dabei Werte zwischen 0% und 100% annehmen. Häufig angewendete Strategien sind bspw. Anforderungsüberdeckung, Anweisungsüberdeckung, Zweigüberdeckung, Bedingungsüberdeckung sowie Parameterüberdeckung. In der Automobilindustrie verbreitet sind spezifische Abwandlungen und Erweiterungen der Metrik [24] [25], diese ergänzen zumeist die präsentierten Methoden um Testfälle basierend auf Erfahrungswissen.

2.4.4.3 Model/SW-Testing (MiL/SiL) – Bestandteil Ansatz III

Entsprechend dem Ansatz des Projektes VVMethoden waren zwei Hauptanwendungen von Modell- bzw. Softwaretests relevant.

1. Verhaltensexploration in der Kritikalitätsanalyse. Dies ist ein MiL-Test, wobei das Fahrzeug inklusive aller seiner Komponenten als insgesamt ausführbares Modell vorliegt. Das Modell umfasst den Bereich „Gesamtfahrzeug“ nach Abbildung 6. Dabei kann die interne Architektur des Modells von der Darstellung abweichen.

2. Validierung der Steuerungsfunktion des Fahrzeugs. Hier ist das Testobjekt der Bereich „Funktion“ nach Abbildung 7. Dabei wird die Produktsoftware getestet. Es handelt sich dann um einen SiL-Test.

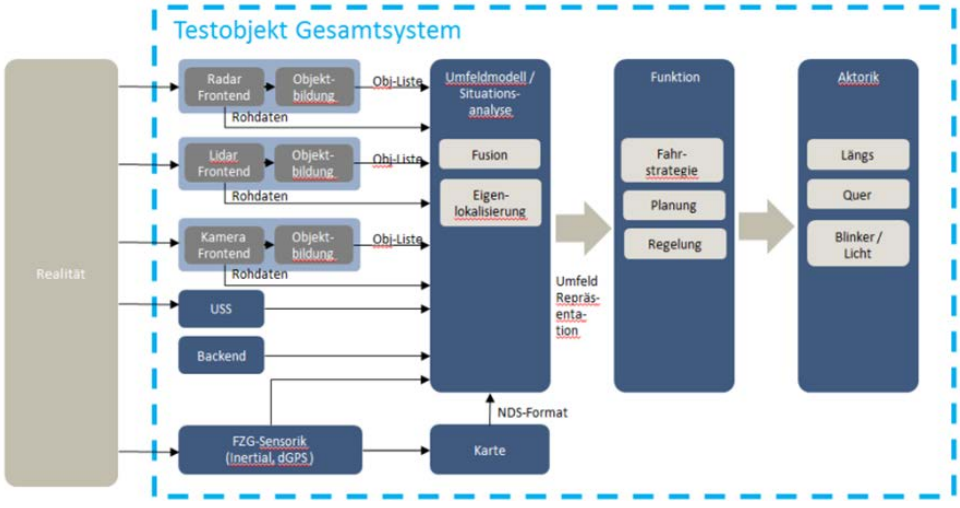


Abbildung 6: Testobjekt Gesamtfahrzeug (Darstellung aus PEGASUS, Testkonzept)

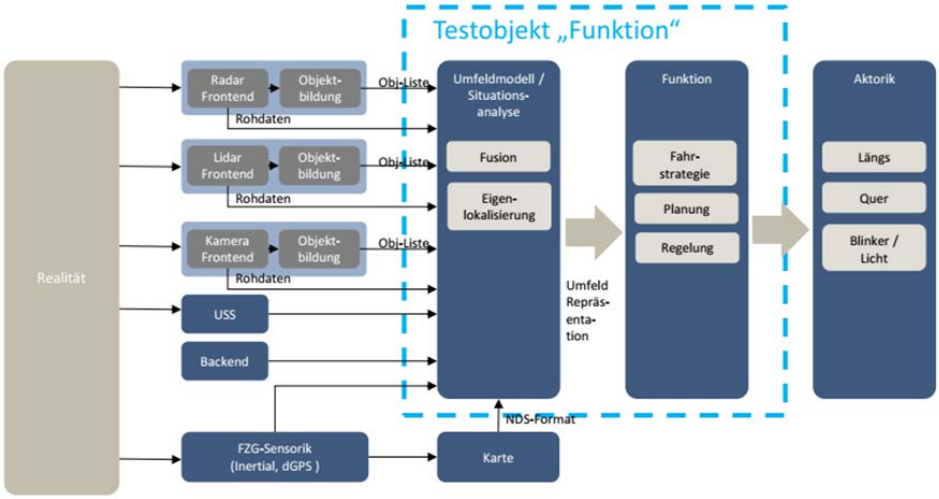


Abbildung 7: Testobjekt Fahrfunktion (Darstellung aus PEGASUS, Testkonzept)

Herstellerintern werden bei der Entwicklung weitere MiL- und SiL-Tests im Entwurfsprozess durchgeführt – z.B. eine Validierung von Modellen der Steuerungsfunktion, also eine MiL-Version des zweiten Anwendungsfalles. Da solche Tests aber stark von der herstellerspezifischen Ausgestaltung des Entwurfsprozesses abhängen, wurden sie in VVMethoden nicht näher betrachtet.

Konzeptionell gibt es keine großen Unterschiede zwischen MiL- und SiL-Tests. Letztendlich ist auch ein ausführbares Modell eine Softwarekomponente. Gemeinsam ist beiden auch, dass in der Testumgebung die Umweltdaten („Realität“) bereitgestellt und die Fahrzeugaktionen dort eingespielt werden müssen. Unterschiede bestehen allerdings in den technischen Randbedingungen und natürlich in den Anwendungsinstanzen im Projekt. Ein Modell, das einem MiL-Test unterzogen werden soll, ist in der Regel für diesen Zweck ausgelegt. Bei Produktsoftware ist dies (nur) dann gegeben, wenn die Simulationsarchitektur bei der Entwicklung berücksichtigt wurde. Kompatibilitätsaspekte haben hier eine Rolle gespielt und mussten zumindest herstellerintern berücksichtigt werden.

Neben pragmatischen Aspekten wie Verfügbarkeit, Lizensierung etc. bestimmen im Wesentlichen folgende Gesichtspunkte, inwieweit Simulationslösungen den Erfordernissen entsprechen.

1. **Interne und externe Schnittstellen der Simulation**. In der Automobilindustrie ist der FMI-Standard (Functional Mock-up Interface, [26] für Simulationskomponenten bereits weit verbreitet. Speziell für Sensormodellierung gibt es das Open Simulation Interface (OSI [27]). Es war zu erwarten, dass zukünftig Simulationslösungen, die auf diesen Standards aufsetzen, das Feld dominieren werden. Bei den externen Schnittstellen ging es um die Testansteuerung inklusive der Testfälle und die Testergebnis-Bereitstellung.

2. **Zeitmodell der Simulation**. Idealerweise sollte eine Simulation so schnell ablaufen können, wie es die Ausführungsrechner erlauben. Dies erfordert jedoch, dass alle Komponenten entsprechende Zeitmodelle unterstützen. Insbesondere die Produktsoftware kann aus technischen Gründen auf eine Simulation unter Echtzeitbedingungen angewiesen sein. Das kann zu Problemen führen, wenn z. B. aufwendige Sensormodelle nicht echtzeitfähig sind.

3. **Realitätstreue bzw. Validität der Simulationsergebnisse**. Zu Projektbeginn waren weder Komponentenmodelle noch Umgebungsrepräsentationen ausreichend realistisch, als dass die Simulationsläufe stets präzise genug die realen Abläufe nachgebildet hätten.

4. **Höhere Simulationssteuerung**. Aufgrund der großen Testräume (in beiden Anwendungsfällen) war eine Teilautomation der Exploration des Verhaltensraumes notwendig. Dies konnte nur über eine enge Verzahnung der Testfallgenerierung mit deren Ausführung und Bewertung geschehen. Für dabei anzuwendende Algorithmen und Verfahren existierten vor Projektbeginn nur Konzepte, die weder detailliert für den praktischen Einsatz ausgearbeitet noch dort erprobt waren.

2.4.4.4 Gerätetest (HiL) – Bestandteil Ansatz III

Hardware-in-the-Loop (HiL) definiert den Einsatz einer Simulationsumgebung für die Ausführung und den Test der in die Zielhardware integrierten Softwarekomponente unter Verwendung der technischen Systemschnittstellen [16]. Auf HIL-Ebene wird zwischen Komponenten- und Integrationstests unterschieden. Beim Komponententest wird die korrekte Funktion eines individuellen Steuergeräts geprüft. HiL-Tests auf Komponentenebene verifizieren die korrekte Interaktion mit der elektrischen und mechanischen Hardware der Systemkomponente (bspw. Motorsteuergerät am Motorenprüfstand). Ein Integrationstest bspw. an einem Wirkkettenprüfplatz dient der Verifikation eines zusammenhängenden und verteilten Subsystems (bspw. Systemverbund Fahrerassistenz) - am Gesamtfahrzeugprüfplatz wird das Zusammenspiel aller im Fahrzeug enthaltenen E/E-Systeme verifiziert.

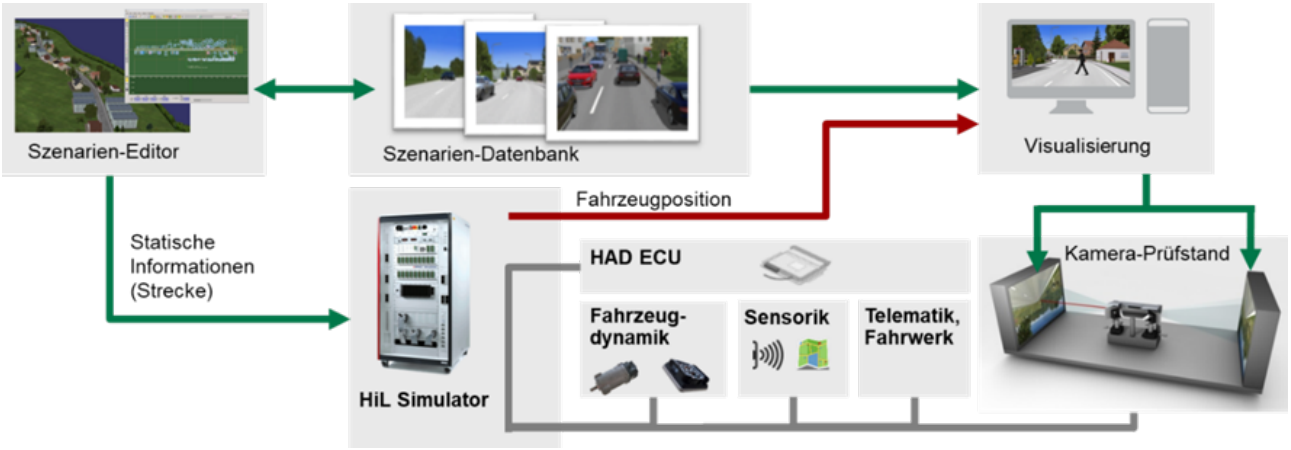


Abbildung 8: Schematische Beispielübersicht für die systematische Absicherung am FAS-Cluster-HiL [28]

In Abbildung 8 ist eine schematische Beispielübersicht für einen Systemverbund-HiL für Fahrerassistenzsysteme auf dem technischen Stand vor Projektbeginn abgebildet. Die reale Hardware ist hierbei einerseits das Steuergerät, auf welchem die Fahrerassistenzsysteme laufen, zudem ist die Fahrzeugdynamik sowie Teile der Sensorik (bspw. Frontkamera) ebenfalls als Hardware in Steuergeräten vorhanden. In einem zugehörigen HiL-Simulator wird nun die restliche Buskommunikation, welche für den korrekten Betrieb der in Hardware verfügbaren Steuergeräte in Echtzeit, simuliert. Hierbei werden die realen Systemschnittstellen (bspw. CAN, FlexRay, Ethernet) verwendet. Für reaktive Regelungssysteme wie beispielsweise einen Abstandsregeltempomat oder teilautomatisierte/hochautomatisierte Systeme muss auch die Regelstrecke für einen Closed-Loop-Test in der Simulation abgebildet sein [20]. Für Open-Loop-Systeme (bspw. Bildverarbeitungssysteme), welche keine Rückführung von Informationen beinhalten, ist keine Abbildung einer Regelstrecke notwendig.

Für die Erweiterung von HiL-Systeme in Richtung Fahrerassistenzsysteme wurden, neben der klassischen Simulation von Restbussen, zur Teststeuerung Fahrzeugsimulatoren wie Virtual Test Drive [29] oder CarMaker [30] angebunden. Diese ermöglichten die virtuelle Fahrt eines Fahrzeugs auf einer simulierten Strecke. Zudem konnten auch weitere Objekte im Umfeld des Testobjekts gesteuert und simulativ abgebildet werden. Verschiedene Szenarien-Datenbanken über mögliche Streckenabschnitte waren in einer Datenbank hinterlegt. Der HiL-Simulator erhilet die statischen Informationen über die Strecke eingespielt und gab die aktuelle Position des Ego-Fahrzeugs zurück, um daraus die Visualisierung der weiteren Verkehrsteilnehmer bzw. der Streckenumgebung zu ermöglichen. Somit konnten zum Test von Umfeldsensoriken auch weitere Verkehrsteilnehmer in die Simulation einbezogen werden. Zum Einspielen der Sensorinformationen über das Umfeld existierten verschiedene Ansätze [31]. Einerseits konnte diese direkt auf Objektebene erfolgen. Basierend auf der Position des Ego-Fahrzeugs wurden über die Simulation Objektlisten im definierten Format, welche zumeist aus einer Sensorverarbeitung kommen, wieder für die Steuergeräte eingespielt. Eine weitere Möglichkeit war es, auf Signalebene entsprechende Vorgaben synthetisch zu erzeugen und einzuspielen. In der dargestellten Abbildung ist auch die Kamera und komplette Verarbeitungskette in Hardware abgebildet, diese hat Monitore abgefilmt, auf denen das synthetische Umgebungsbild entsprechend der Ausrichtung eingeblendet wurde. Dies ermöglichte den integrierten Test der Kamera-Hardware.

Der HiL-Test wird als systematischer Test beschrieben. Im Rahmen einer übergreifenden Teststrategie wird eine Testspezifikation mit Testfällen erstellt. Die Testfälle orientieren sich zumeist an einer Abdeckung sämtlicher Anforderungen [24], auch andere Arten der Abdeckung können berücksichtigt werden. Systematischer Test heißt, alle zu testenden Fälle werden im Voraus definiert. Die Testfallbeschreibung erfolgt in folgendem Schema. Zunächst werden alle Vorbedingungen und Initialisierungen, welche für den Betrieb des Systems bzw. für das Bringen des Testobjekts in einen bestimmten Zustand benötigt werden, definiert. Im Anschluss erfolgt ein Event bzw. Aktion, (z.B. veränderter Signalwert, steigende Flanke,…) um das Testobjekt zu stimulieren [31]. Im letzten Schritt wird nun die Reaktion des Testobjekts auf die Stimulation angeschaut und gegenüber einer vorab ausgedrückten Erwartungshaltung (definiert bspw. in der Anforderung) überprüft. Eine binäre Auswertung (PASS/FAIL) erlaubt die einfache Auswertung des Testfalls.

2.4.4.5 Testen im Fahrzeug – Bestandteil Ansatz III

Testen im virtuellen Bereich konnte insbesondere bei regelnden Funktionen nicht das tatsächliche Fahrerlebnis in einer realen Umgebung ersetzen. Für die Validierung in realen Umgebung wurde in frühen Entwicklungsphasen das Rapid Prototyping mit umgebauten Versuchsträgern auf Basis hoch performanter Prototypensteuergeräte verwendet [17]. In späteren Phasen wurden Konzeptfahrzeuge, Erprobungsträger und Dauerläufer mit der realen Zielhardware genutzt. Um eine entwicklungsbegleitende Validierung zu ermöglichen, wurden Erprobungsträger mit unterschiedlichen Musterständen der Steuergeräte ausgerüstet [25]. Die Musterstände ermöglichten eine sukzessive Integration von Funktionen im Laufe der Entwicklung. Am Ende der Entwicklung wurde die Produktions- und Verkaufsfreigabe basierend auf den Ergebnissen der Test- und Qualifikationsphasen erteilt. Die Freigabe beinhaltete zudem die Ergebnisse von Winter- und Sommererprobungen sowie länderspezifischen Erprobungen [32].

Im realen Fahrversuch wurden Fahrzeuge unter spezifizierten Bedingungen im realen Betrieb getestet. Die durch professionelle Testfahrer durchgeführten Fahrversuche basierten dabei auf definierten Prüfkataloge [33]. Die Prüfung durch den Fahrversuch erfolgte sowohl auf öffentlichen Straßen, als auch auf dezidierten Prüfgeländen. Insbesondere die Validierung von sicherheitskritischen Fahrfunktionen wurde auf dezidierten Prüfgeländen durchgeführt, deren Verfügbarkeit sehr begrenzt ist [34]. Die Prüfkataloge basierten zumeist auf Erfahrungswissen bspw. aus vorherigen Baureihen sowie der Expertise des Ingenieurs. Hierbei wurde das Fahrzeug stets in einen definierten Ausgangszustand gebracht und anschließend Manöver beschrieben, welche der Testfahrer durchzuführen hatte. Am Ende des Manövers erfolgte die Auswertung subjektiv durch den Testfahrer, das Ergebnis wurde entsprechend dokumentiert. Zudem waren im Rahmen von Prototypenfahrzeugen sowie Erprobungsträgern zumeist Datenlogger verbaut, welche sämtliche Informationen aufgezeichnet haben. Diese haben es erlaubt, sich kritische Situationen nochmals im Labor anzuschauen und mögliche Ursachen zu identifizieren.

2.5 Zusammenarbeit mit anderen Stellen

Das Projekt VVMethoden hatte zwei wesentliche externe Anschlüsse: Einerseits hat es stark auf den Ergebnissen von PEGASUS aufgebaut. Andererseits war der Austausch mit einem weiteren teilweise parallel laufenden Projekt fest eingeplant – SET Level 4to5. Außerdem konnte auf Vorarbeiten von Projektpartnern zurückgegriffen werden und das Projekt hat aktiv den Austausch mit externen Partner gesucht. Diesa Aktivitäten wurden hauptsächlich über das TPX organisiert und ist in Kapitel 3.1.2.10 näher ausgeführt. Aus diesem Grund wird hier vor allem die VDA Leitinitiative autonomes und vernetztes Fahren dargestellt sowie die Einbindung von VVM in die Projektfamilie.

2.5.1 VDA Leitinitiative autonomes und vernetztes Fahren

Der globale Wettbewerb mit kapitalkräftigen neuen Marktteilnehmern und die rasante Digitalisierung nicht nur der Mobilität erfordern eine noch nie da gewesene Innovationsgeschwindigkeit und enorme Investitionen in Forschung und Entwicklung. Die Antwort der VDA Leitinitiative darauf lautet: Kooperation. Durch intensiv vernetzte Großprojekte und erhöhte Transparenz in der vorwettbewerblichen Grundlagenforschung zielt die VDA Leitinitiative auf einen breiten Kompetenzaufbau in den zentralen Schlüsseltechnologien für AVF am Standort Deutschland.

Innerhalb der Leitinitiative diskutieren und entwickeln die beteiligten Industriepartner eine gemeinschaftliche Position zu Forschungs- und Entwicklungsbedarfen. Die Politik kann auf diese abgestimmte Industrieposition zurückgreifen und Förderschwerpunkte entsprechend ausrichten. Durch intensive Zusammenarbeit mit den relevanten Bundesministerien ist es der Leitinitiative gelungen, die Kohärenz in der Ausrichtung der nationalen Förderpolitik für AVF zu stärken und die Konvergenz in der Technologieentwicklung programm- und projektübergreifend zu erhöhen. Die Mitglieder der VDA Leitinitative identifizieren und erarbeiten gemeinsam die wichtigen Themen- und Handlungsfelder für die Entwicklung des AVF. Als Koordinierungsstelle initiiert leitet sie große, beteiligungsoffene Kosnortialprojekte. So wurden seit der Gründung der Leitinitiative im Herbst 2016 bereits wichtig Großprojekte mit einem industrie- und forschungsübergreifenden Partnernetzwerk auf den Weg gebracht.

Ausgelegt in Form von Projektfamilien werden Forschungs- und Entwicklungsressourcen effizient eingesetzt. Innerhalb der Projektfamilien werden bei überschneidenden Anforderungen und Forschungsinhalten Synergien zwischen Projekten gehoben und Ergebnisse über Projektgrenzen hinweg geteilt. Neue Projekte setzten gezielt auf den Ergebnissen bestehender Projekte auf. So werden Redundanzen und Fehlinvestitionen vermieden und eine hohe Anschlussfähigkeit und Verwertbarkeit der Projektergebnisse ermöglicht.

Die von der Leitinitiative entwickelten Projektfamilien KI Familie, PEGASUS und @City adressieren die für die Wettbewerbsfähigkeit besonders wichtigen Forschungs- und Entwicklungsfelder des autonomen und vernetzten Fahrens. Während in der KI-Familie der Schwerpunkt auf Datengenerierung und sichere Künstliche Intelligenz liegt, drehen sich die Projektarbeiten in der PEGASUS-Familie um Standards für das Testen und die Sicherheitsvalidierung hochautomatisierter Fahrfunktionen. In der @City-Familie steht die Ausweitung der Automatisierung und der Operational Design Domains (ODD) mit dem Schwerpunkt urbaner Verkehr im Mittelpunkt.

2.5.2 PEGASUS Projektfamilie

VVMethoden war Teil der Projektfamilie „Verifikation und Validierung“ der VDA-Leitinitiative autonomes und vernetztes Fahren (PEGASUS-Familie).

Wesentliche Vorarbeiten für die Thematik von VVMethoden wurden im BMWi-geförderten Verbundprojekt **PEGASUS** erarbeitet, das Mitte 2019 beendet wurde. Dort wurde die Absicherung von hochautomatisierten Fahrfunktionen mit der Beispielfunktion Autobahnchauffeur betrachtet und prototypisch erprobt, der in der Lage sein soll, automatisiert ein Fahrzeug unter Normalbedingungen auf der Autobahn zu führen. Solange die Fahraufgabe innerhalb der Systemgrenzen bleibt, muss der Fahrer die Automation nicht überwachen. Der Fahrer kann unter bestimmten Umständen, z. B. beim Erreichen der Funktionsgrenze, zur Übernahme durch die

Funktion aufgefordert werden. Es handelt sich somit um eine Funktion des SAE-Level 3. Zentrales Ergebnis des Projektes war eine Gesamtmethode zur Erbringung des Sicherheitsnachweises der Fahrfunktion. Diese Gesamtmethode wurde exemplarisch realisiert inklusive

- einem umfassenden Testkonzept. Zu diesem gehören
- Analyse von Test- und Messdatenreihen inklusive einer Bewertung von Testergebnissen im Hinblick auf die Sicherheitsargumentation,
- eine Gesamtarchitektur, auf welcher die Methode realisiert werden kann,
- Argumentationsmuster für einen Sicherheitsnachweis.

Diese Methode wurde zwar zunächst anhand der Anwendung auf den Autobahnchauffeur entwickelt, hatte aber den Anspruch, als Vorlage auch für andere Funktionen verwendbar zu sein. Dies wurde in VVMethoden weiterentwickelt.

Zeitlich weitgehend parallel VVMethoden wurde ein weiteres Projekt aus dieser Familie durchgeführt, **SET Level 4to5**. Dort wurden Simulationsmethoden und -technologien entwickelt, die im Projekt VVMethoden eingesetzt werden konnten, während in VVMethoden wiederum Anforderungen erarbeitet wurden, die SET Level 4to5 zur Verfügung gestellt wurden.

Eine Zusammenarbeit der beiden Projekte hat die Effizienz in der Erreichung des übergeordneten Ziels beider Projekte erhöht: Da Informationen und Ergebnisse kontinuierlich während der Laufzeit der beiden Projekte ausgetauscht wurden, konnten die Erkenntnisse zum Testen von L4/L5-Systemen für den Einsatz im urbanen Umfeld zusammen mit Simulationsmethoden und -technologien schrittweise entwickelt und verfeinert werden (Kosten- und Zeiteffizienz).

Inhaltlich war in VVMethoden ein spezielles Teilprojekt (TP5) definiert, das die Simulationsplattform bereitgestellt und die Verbindung mit SET Level 4to5 hergestellt hat. Im SET Level 4to5 Projekt wurden die Simulationsmethoden sowohl für die Kritikalitätsanalyse als auch für die Testumgebung entwickelt. Das VVMethoden Projekt wiederum hat die Umgebung bereitgestellt, in der die Einsatzfähigkeit der Simulationsmethoden geprüft und verifiziert werden konnte.

Ein kontinuierlicher Austausch der fast parallel laufenden Projekte hat die Möglichkeit geboten, die Wirkung der beiden Projekte noch einmal deutlich zu steigern. Um jenseits der Einzelergebnisse dieses zusätzliche Potential zu heben, waren die relevanten Schnittstellen bzw. Austauschpunkte für den Ergebnistransfer zwischen den Projektpartnern beider Konsortien abgestimmt worden.

In VVMethoden war es Teil der Projektmanagement-Aufgabe den Austausch zwischen den Projekten zu koordinieren. Mögliche oder nötige Adaptionen in der geplanten Zusammenarbeit wurden mit SET Level 4to5 abgestimmt und dann umgesetzt. Der Arbeits- und Zeitplan wurde in beiden Projekten so eingelöst, dass die identifizierten Potentiale mobilisiert werden konnten. Bei Zielkonflikten hatten die Einzelinteressen von VVMethoden hier naturgemäß den höheren Stellenwert. Für das Projektmanagement von VVMethoden bedeutete dieser angestrebte und über die herkömmliche Kooperationspraxis hinausweisende Bezug eine zusätzliche Messgröße in der Fortschritts- und Ergebnisbewertung und wurde in die periodische Statusberichterstattung auf AP-, TP- und Gesamtprojektebene einbezogen.

Da in den beiden Konsortien eine hohe Überschneidung der Partner vorhanden war und beide Projekte in den Rahmen der VDA Leitinitiative eingebunden waren, bestand ein hohes Interesse an der hier beschriebenen Potentialmaximierung, so dass das Risiko eines solchen Außenbezugs begrenzt war. Hätten Ergebnisse aus SET Level 4to5 nicht in dem vorgesehenen Ausmaß in VVMethoden eingebracht werden können, so war vorgesehen, die fehlenden Beiträge in angemessener Form über die vorhandenen Simulationskompetenzen der beteiligten Häuser und Wissenschaftspartner auch unter Nutzung weiterer laufender Aktivitäten wie „SmartSE“ darzustellen. In diesem Fall wäre eine Bündelungsfunktion der Simulationsaspekte in TP9 durch Aufnahme und Bewertung der Simulationsansätze der Industriepartner erfolgt. In TP5 wäre dann entsprechend die Koordination der Simulationsansätze erfolgt. Dies war allerdings nicht der Fall und der beabsichtigte Synergiegewinn konnte erreicht werden.

2.5.3 Offene Treffen zur Ergebnisverbreitung

Das Konsortium hatte einen umfassenden Austausch mit externen Stakeholdern geplant. Hierfür notwendige Ressourcen wurden in den jeweiligen Teilprojekten abgebildet sowie Gegenstand der Unterbeauftragung eines Projektbüros. Mit Blick auf die definierte Ergebnisdokumentation hat es sich aus Sicht des Konsortiums angeboten, konkrete Ergebnisse definierten Stakeholder-Gruppen vorzustellen und zu diskutieren.

Durch die Projektstruktur mit drei Iterationsphasen lagen zu drei Zeitpunkten konsolidierte Ergebnisse vor, die sich hauptsächlich in den verwendeten Daten und den Reifegraden der Methodenentwicklung unterschieden haben. Um eine zeitnahe Übernahme der Projektergebnisse in die industrielle Wertschöpfungskette zu ermöglichen, wäre es sinnvoll gewesen, die entwickelten Konzepte und ihre technische Umsetzung zu allen drei Zeitpunkten der Fachöffentlichkeit vorzustellen. Die hätte bei den geplanten offenen Treffen zur Ergebnisverbreitung stattfinden sollen, die jeweils am Ende der Iterationsphasen geplant waren, und damit in den Quartalen 8, 12 und 48 (siehe Abbildung 54). Aufgrund der Covid19-Pandemie konnte nur das erste dieser Treffen als Vor-Ort-Veranstaltung durchgeführt werden. Die verbleibenden zwei Treffen wurden dann als Onlineveranstaltung unter Nutzung eines geeigneten Tools durchgeführt (s. Kapitel 3.1.2.9).

Die entsprechenden Inhalte wurden in den öffentlich zugänglichen Deliverables 03, 06 und 11 präsentiert.

3 Eingehende Darstellung

3.1 Erzielte Ergebnisse

3.1.1 Die Gesamtmethode

3.1.1.1 Methodischer Rahmen

In diesem Kapitel wird der methodische Rahmen der VVM-Gesamtmethode beschrieben. Als direktes Nachfolgeprojekt des Projektes PEGASUS, wird zunächst die PEGASUS-Gesamtmethode vorgestellt. Die Aufgabe des Projektes VVM war es, diese insbesondere für automatisierte Fahrsysteme des SAE-Levels 3 bis 4 weiter zu entwickeln.

Analog zu PEGASUS hatte auch das Projekt VVM vom Projektträger den Auftrag, die internationale Kommunikation von PEGASUS aufrecht zu erhalten und sich in die Abstimmung von Standards, Normen und entstehenden Regularien, insbesondere in Kontext der UN, aktiv einzubringen Auch diese Aktivitäten werden in diesem Kapitel vorgestellt.

VVM hatte den Auftrag für die Projekte der PEGASUS-Familie auf die gemeinsame Fachsprache dieser Projekte zu achten und bei Dissonanzen, an einem Ausgleich der Begriffswelt zu arbeiten. Die Vorgehensweise und die erzielten Ergebnisse finden sich am Ende des Kapitels.

3.1.1.1.1 Aufsatzpunkt PEGASUS

Das Forschungsprojekt PEGASUS (**P**rojekt zur **E**tablierung von **g**enerell **a**kzeptierten Gütekriterien, Werkzeugen und Methoden sowie **S**zenarien **u**nd **S**ituationen zur Freigabe hochautomatisierter Fahrfunktionen) war in den Jahren 2016 bis 2019 angetreten, die Freigabeherausforderung für hochautomatisierte Fahrzeuge des SAE-Level 3 zu bearbeiten. Hierzu arbeiten im Rahmen des vom Bundesministerium für Wirtschaft und Klima geförderten Forschungsprojektes Partner aus der Industrie und Wissenschaft zusammen, darunter Automobilfirmen, Zulieferer, Prüfeinrichtungen sowie Forschungseinrichtungen. Ziel war es, einen herstellerübergreifenden Prozess zu definieren, um die Sicherheit von hochautomatisierten Fahrfunktionen (SAE Level 3) nachzuweisen [35].

Schon während der Anbahnung des PEGASUS Projektes [36] bis 2016, welches die Keimzelle der heutigen Projekte der PEGASUS-Projektfamilie war, herrschte in der Automobilbranche eine große Übereinstimmung, dass neue technologische Wege für die Entwicklung und Validierung automatisierter Fahrsysteme jenseits reiner distanzbasierter Ansätze benötigt werden. Bei der Nutzung der konventionellen statistischen Methoden wären Milliarden von Testkilometern für Test und Freigabe hochautomatisierter Fahrzeuge erforderlich gewesen [37], um die vor Beginn des Projektes Methoden nach dem Stand der Technik etablierten Vorgehensweisen zu adaptieren. Um diese Herausforderungen zu bewältigen, schlug das PEGASUS Projekt drei Hauptpfeiler vor:

- Initiierung einer szenariobasierten Entwicklung und Erprobung.
- Förderung und Entwicklung von simulativen Ansätzen, die den gesamten Prozess abdecken.
- Entwurf und Aufbau von Szenario-Datenbanken.

Als Projektergebnis ergab sich eine Gesamtmethode, die auf fünf Bausteinen bestand. Diese sollen kurz vorgestellt werden.

Abbildung 9: PEGASUS - Übersicht über das Projekt [35]

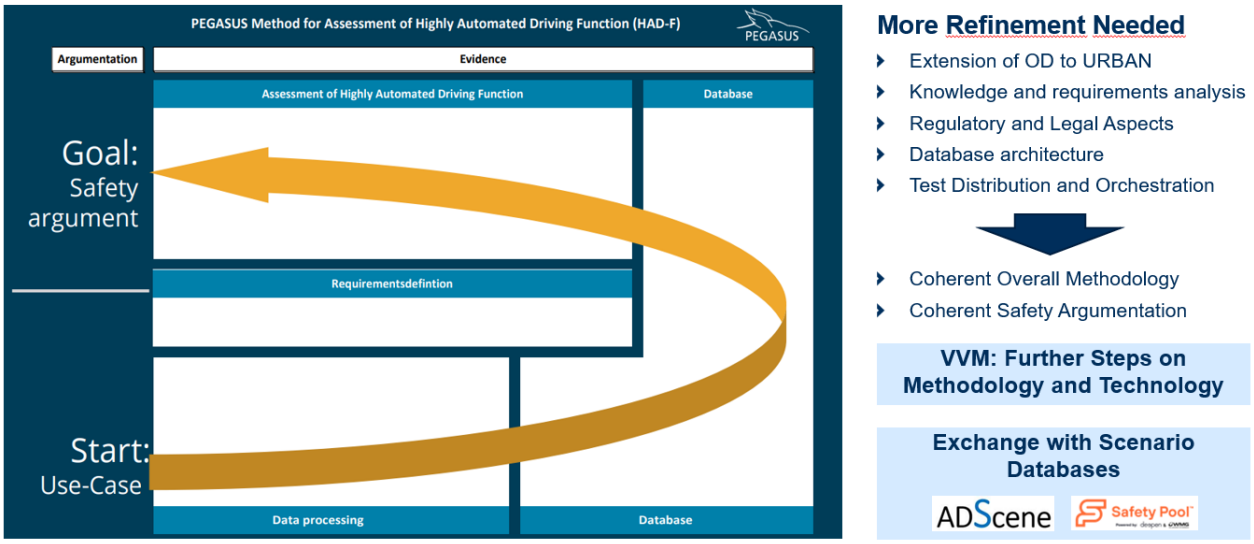


Abbildung 10: Aufsatzpunkt PEGASUS-Methode [35]

(1) Szenarienermittlung

Ziel des ersten Prozessbausteins -der *Szenarioidentifikation*- ist die die systematische Generierung funktionaler sowie daraus abgeleitet logischer Szenarien. Es wird dabei daten- und wissensbasiert vorgegangen.

Beim wissensbasierten Vorgehen werden die Szenario-Klassen aus Expertenwissen, Gesetzen, Standards, Normen und Richtlinien sowie insbesondere einer systematischen Untersuchung von Automationsrisiken abgeleitet (siehe Abbildung 11Abbildung 11: Identifikation von Automationsrisiken (Klasse 1) in [36]) Die Methoden zur Identifizierung von Automationsrisiken

nutzen bewährte Techniken zur Gefahren- und Risikobewertung sowie eine gründliche Sicherheitsanalyse. Es wird auch die Systemtheoretische Prozessanalyse (STPA) verwendet. Die Analyse der Automationsrisiken dient dem Zweck, die Ursachen von Risiken frühzeitig zu identifizieren, insbesondere jene, die sich aus der Einführung hochautomatisierter Fahrfunktionen (HAF-Funktionen) ergeben. Dadurch können neue Szenarien gefunden werden, die eine potentielle Herausforderung für automatisierte Fahrfunktionen sind. Für die wissensbasierte Identifikation von Szenarien ist beispielsweise eine ontologiebasierte Szenarienermittlung möglich, um alle möglichen Szenarioparameter und deren Einfluss im Szenario strukturiert zu bestimmen. Im Rahmen dieser Arbeiten wird auch die methodische Unfalldatenanalyse eingesetzt. In GIDAS-Daten wird strukturiert der Einfluss unterschiedlicher Szenarioparameter auf das Unfallgeschehen (Schwere und Häufigkeit) ausgewertet.

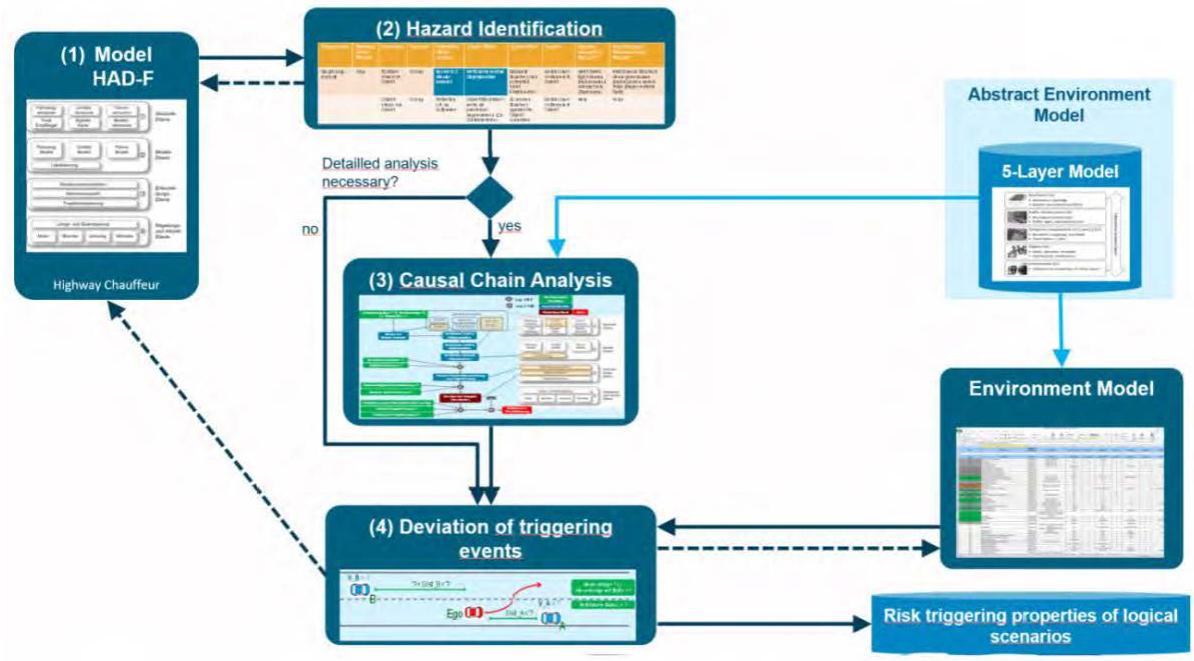


Abbildung 11: Identifikation von Automationsrisiken (Klasse 1) in [36]

Beim datenbasierten Ansatz werden aus Unfalldaten wie z.B. GIDAS, sowie aus Feldtestdaten, Testfahrten, Simulatorfahrten und Simulationsdaten Verhalten der Verkehrsteilnehmer in relevanten Szenarien ermittelt und anhand eines definierten Unfallrisikos (KPI) klassifiziert. ES entstehen risiko-basierte Modelle von relevanten Szenarien.

Die Ergebnisse des wissens- und datengetriebenen Ansatzes definieren von Szenarien und Parameterräume für die Verifizierung und Validierung.

(2) Anforderungsermittlung

Die Anforderungsanalyse verwendet das abstrakte Szenario-Wissen, um technisch verwendbare Anforderungen für die automatisierte Fahrfunktion oder an das Testobjekt zu definieren. In der Anforderungsermittlung wird die Kernfrage bearbeitet, was das automatisierte Fahrzeug mindestens leisten muss. Dazu wurden in PEGASUS zwei Methoden angewendet. Zum einen wurde ein Ansatz entwickelt, der auf gesellschaftlichen Akzeptanzkriterien basiert. Zum anderen wird eine Bewertung mit einem risikobasierten Ansatz durchgeführt.

Hier ist der Vergleich mit der Leistungsfähigkeit des Referenzmaßstabs Mensch wichtig, da automatisierte Fahrzeuge einerseits nicht zu einer Verschlechterung der Verkehrssicherheit führen sollen, andererseits aber auch nicht zu hohe Anforderungen an ihre Einführung eine mögliche Verbesserung der Verkehrssicherheit verzögern dürfen. Zu diesem Zweck wird ein Qualitätsmaß für automatisierte Fahrfunktionen ermittelt, indem die menschliche Leistungsfähigkeit mit der Leistungsfähigkeit automatisierter Fahrfunktionen in kritischen Verkehrssituationen verglichen wird.

Die Anforderungsdefinition erfolgt unabhängig von der Szenariendefinition auf Basis von Erkenntnissen aus Gesetzen, Standards, Normen und Richtlinien. Der Vergleich mit dem Referenzmaßstab Mensch fließt ebenfalls in die Anforderungsermittlung ein. Die Anforderungen werden in einer Metrik gespeichert und später zur Bewertung der Szenarien im Test verwendet, um die Leistungsfähigkeit und Qualität des Systems zu beurteilen. Die Anforderungsermittlung hat im Rahmen der PEGASUS-Methode das übergeordnete Ziel, die Anforderungen an die hochautomatisierte Fahrfunktion auf Basis von abstraktem Wissen aus verschiedenen Quellen zu definieren und Prozessrichtlinien und Metriken für die Bewertung im Entwicklungsprozess und insbesondere für die Validierung und Verifikation bereitzustellen.

(3) Datenbank

In diesem Baustein werden die im Realverkehr erhobenen Datensätze verwendet, um aus den Daten zunächst vordefinierte logische Szenarien und deren Charakteristika (6-Ebenen-Modell) zu identifizieren. Darüber hinaus werden die aufbereiteten Datensätze verwendet, um Parameterräume für verschiedene Szenarienparameter zu definieren. Die Daten werden ergänzt um Unfalldaten sowie Expertenwissen und Szenarien aus Regularien und Gesetzen. In der Summe entsteht ein statistisches Bild der ODD, das als Ausgangsbasis für das szenariobasierte Testen und insbesondere der Evaluierung des Risikos eingesetzt wird. Anhand dieser Informationen erstellt die Datenbank einen Raum von logischen Testfällen mit integrierten Pass- und Fail-Kriterien aus dem zweiten Element für die verschiedenen logischen Szenarien, die die ODD klassifizieren. (siehe Abbildung 12)

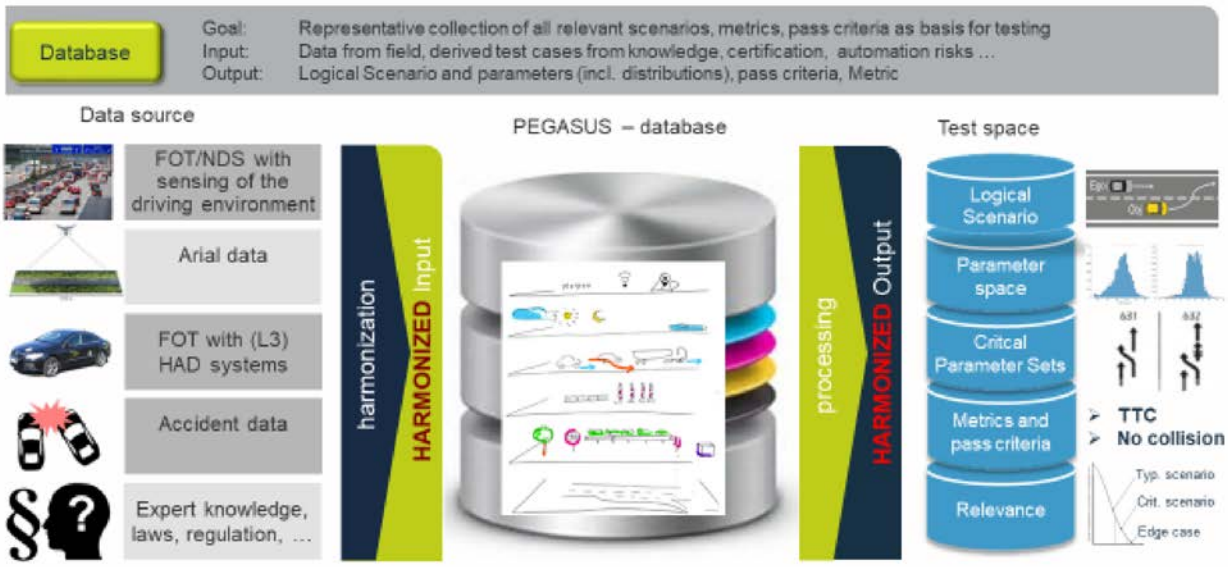


Abbildung 12: Ein zentraler PEGASUS-Baustein: Szenario-Parameter-Datenbank [37] [38].

(4) Bewertung der hochautomatisierten Fahrfunktion

Das vierte Basiselement beinhaltet das szenariobasierte Testen und die Bewertung der Testergebnisse. Basierend auf den relevanten logischen Szenarien und den dazugehörigen Parameterräumen werden Testräume inklusive Akzeptanzkriterien, Evaluierungsfunktionen und Akzeptanzlevel abgeleitet. In Kombination mit den Testzielen und dem V&V-Konzept (siehe Abbildung 13) entstehen hieraus Testfallspezifikationen.

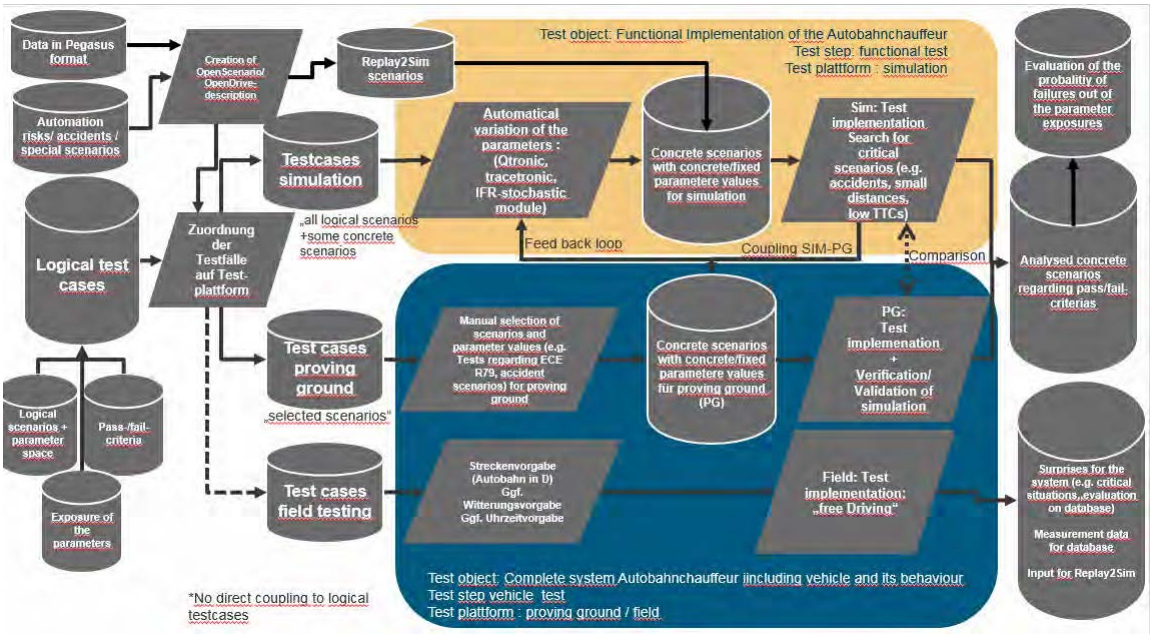


Abbildung 13: Test- / V&V Konzept bei der Evaluierung des Risikos des ADS im Rahmen der PEGASUS-Methodik

Zur Evaluierung des Risikos der Integration eines ADS in ein Fahrzeug in der ODD folgt das Vorgehen einem integrierten Testkonzept mit mehrstufigem Dekompositionsansatz. Im nächsten Prozessschritt werden die konkreten Testfälle in Abhängigkeit von dem Testlevel in der Simulation (Testinstanzen von MiL über HiL-Varianten bis ViL) sowie auf Prüfgeländen ausgeführt und durch Erprobungen während der Realfahrt ergänzt. Der erste Schritt beinhaltet eine Simulation der erstellten Testfallspezifikationen. Mithilfe der Simulation erfolgt eine Identifikation der Grenzen von Unfallschweren (S0 bis S3) in den Parameterräumen eines logischen Szenarios sowie eine Bestimmung von Repräsentanten von Äquivalenzklassen. In diesem Zusammenhang werden im Simulationsframework (Abbildung 14), welches auch die Distribution auf diverse Soft- und Hardware-in-the-Loop-Testinstanzen einbezieht, Variationsmethoden eingesetzt [39]. Für eine Auswahl von Parametern erfolgt eine Variation der Parameter mit stochastischer Wahrscheinlichkeit und nachfolgende Durchführung als Black-Box-Test. Es werden so Versagenswahrscheinlichkeiten des ADS bestimmt. Anhand der Akzeptanzkriterien lässt sich feststellen, ob der Test bestanden ist. Testfälle, die nicht oder nur knapp bestanden wurden, werden mit den identifizierten Repräsentanten für Äquivalenzklassen auf dem Prüfgelände überprüft. Ziel der Evaluierung ist die Einhaltung einer positiven Risikobilanz mit Vorgaben an eine Systemperformanz (Referenzfahrer), zu überprüfen. Die Performanzvorgaben stellen sicher, dass das automatische Fahrsystem Mindestanforderungen an eine sichere Kontrollierbarkeit von Szenarien, die in der ODD auftreten können, gewährleistet. Das Performance-Ziel für das ADS ist: „Das automatische Fahrsystem muss in der Lage sein, jedes Szenario in der ODD statistisch mindestens ebenso gut zu beherrschen, wie ein (statistischer) menschlicher Referenzfahrer."

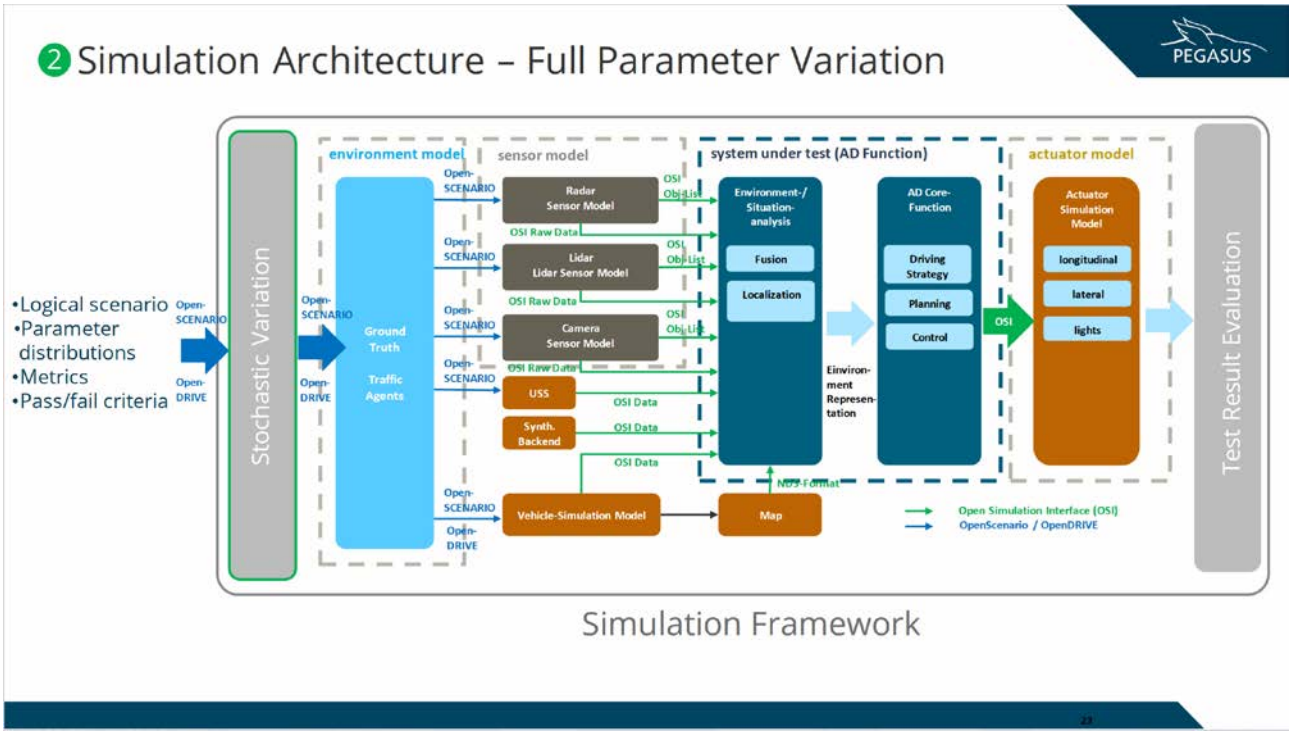


Abbildung 14: Simulationsframework PEGASUS im Rahmen der Gesamtmethode [39]

Feldtests im realen Straßenverkehr sind hingegen für das kontrollierte Testen des ADS in Parameterräumen logischer Szenarien ungeeignet. Sie dienen dazu, unerwartete Effekte zu identifizieren und dadurch die Robustheit des Systems zu verbessern. Das Verhalten des Gesamtsystems wird insbesondere im Hinblick auf seine Resilienz gegenüber einem stochastischen Kontext untersucht. In Ergänzung zu den bestehenden Defiziten von Sensormodellen wird eine Kombination aus Prüfgelände- und Feldtest durchgeführt, um die Verifikation und Validierung zu stützen. (Siehe hierzu Abbildung 13).

Im Rahmen der Bewertung von hochautomatisierten Fahrfunktionen erfolgt abschließend eine Bewertung der ermittelten Testergebnisse sowie eine Risikoermittlung anhand vordefinierter Verhaltensweisen. Diese beinhalten:

(a) die *Einhaltung angemessener Sicherheitsabstände*,

(b) die *Verhinderung* bzw. (c) die *Abmilderung der Schwere von Kollisionen*

(d) die *Kontrollierbarkeit jedes Szenario durch das ADS statistisch mindestens ebenso gut, wie ein(statistischer) menschlicher Referenzfahrer.*

(5) Sicherheitsargumentation

Der fünfte Baustein der PEGASUS-Methodik besteht in der Erstellung einer Sicherheitsargumentation. Das Ergebnis basiert auf einen strukturierten und formalisierten Ansatz der Argumentation (siehe Abbildung 15) und soll einen Nachweis der Sicherheit und Leistungsfähigkeit des ADS (beispielhaft der in PEGASUS untersuchte Autobahn-Pilot) dienen. Die Sicherheitsargumentation ist in fünf Ebenen aufeinander aufbauenden Ebenen formuliert, die eine Rückverfolgbarkeit von jedem Ergebnis einer höheren Ebene auf die Ziele der niedrigeren Ebenen ermöglicht.

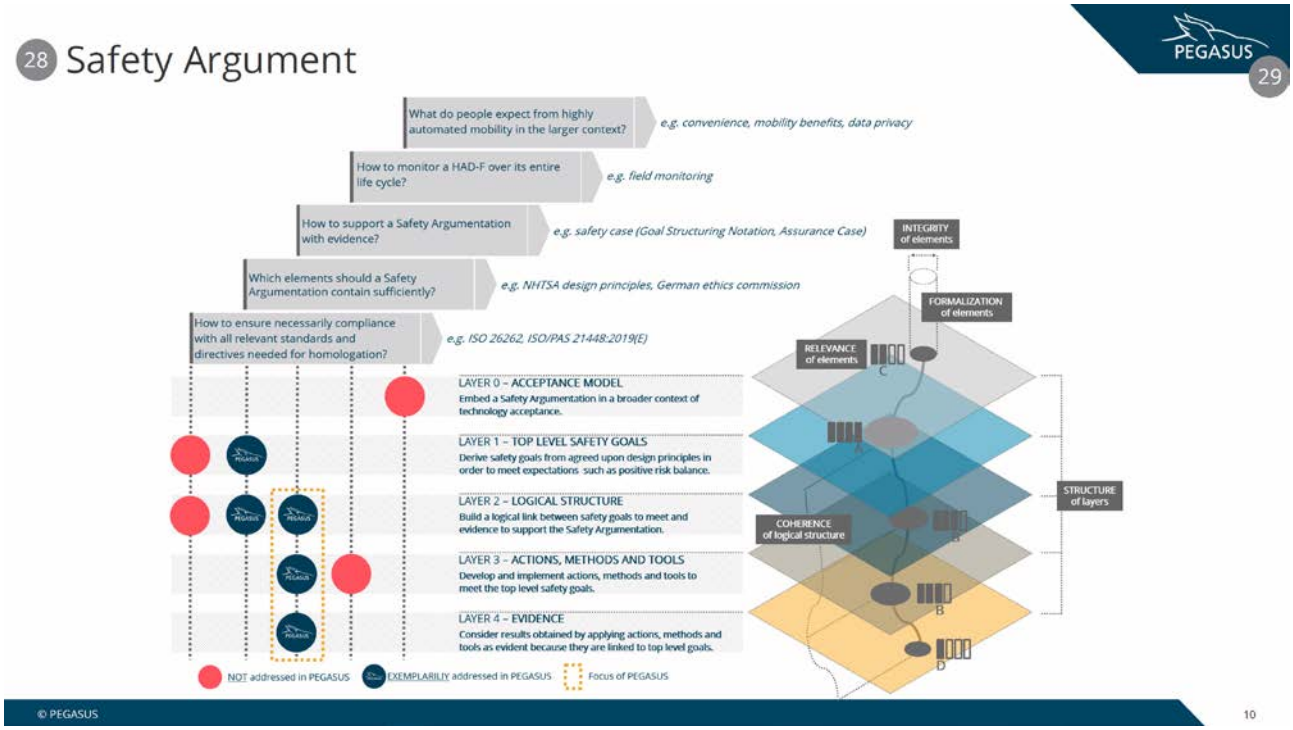


Abbildung 15: Sicherheitsargumentation auf Basis PEGASUS-Methodik [36] [40] [41]

Das Argumentationsschema (Abbildung 15) beginnt dabei auf Ebene 0, dem sogenannten Akzeptanzmodell, das die individuelle und gesellschaftliche Akzeptanz hochautomatisierter Funktionen anhand eines wissenschaftlichen Modells beschreibt. Daraus folgt in Ebene 1 die Ableitung übergeordneter gesellschaftlicher Sicherheitsziele wie sie beispielsweise aus dem Bericht der deutschen Ethikkommission zum automatisierten und vernetzten Fahren abgeleitet werden können. (für Deutschland insbesondere eine positive Risikobilanz mit Fahrerleistungsreferenz) Auf Ebene 2, der logischen Struktur, werden nun daraus konkrete Sicherheitsziele definiert. Diese konkreten Sicherheitsziele beschreiben, welche Ergebnisse für den Nachweis der Sicherheit und Zuverlässigkeit relevant sind. Ebene 3 definiert, wie der Nachweis so erbracht wird, dass die konkreten Sicherheitsziele aus Ebene 2 erreicht werden. Dieser Nachweis wird mit der PEGASUS-Methode geführt. Auf der Ebene 4, der Evidenz, wird untersucht, welchen Beitrag das jeweilige Ergebnis der PEGASUS-Methode zur Erreichung eines konkreten Sicherheitsziels leistet.

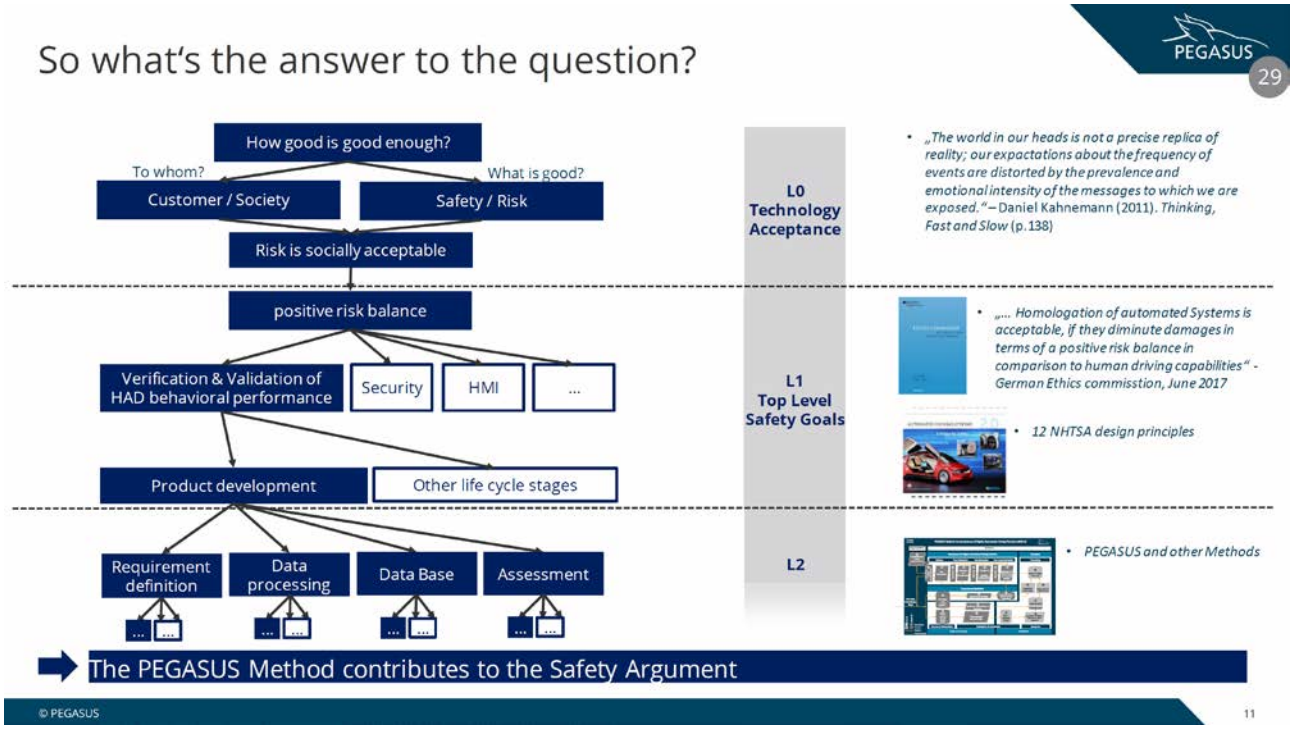


Abbildung 16: Struktur der Sicherheitsargumentation von PEGASUS [36] [40] [41].

Eine Einbindung der PEGASUS-Methode in den Entwicklungsprozess zeigt Abbildung 17.

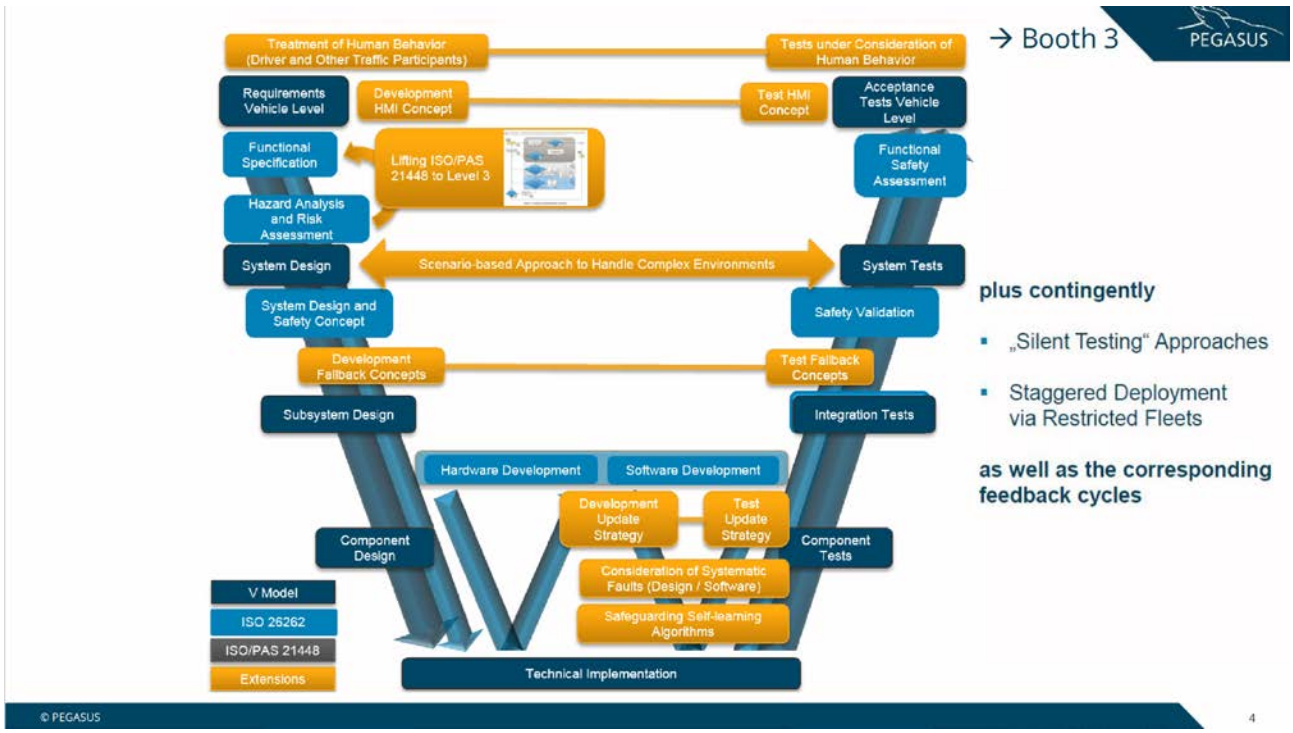


Abbildung 17: PEGASUS-Methode im V-Modell [42]

Um diese Ziele zu erreichen, hat das Projekt PEGASUS [36] an der Erstellung von allgemein akzeptierten Qualitätskriterien, Werkzeugen und Methoden sowie an Szenarien und Situationen gearbeitet. Von Anfang an waren die Arbeiten in einen offenen, internationalen Ansatz eingebettet:

Der Ansatz zielte auf die Verbreitung der PEGASUS-Idee in der globalen Automobil-Community, sowohl bei der Industrie als auch bei Forschungsinstituten. Gleichzeitig diente ein kleineres, spezielles Format, die PEGASUS-Experten-Workshops, dem Austausch zu Themen von hohem Interesse für die Automobilindustrie und den akademischen Partnern.

Das PEGASUS-Projekt schaffte eine enorme internationale Vernetzung mit Ministeriumsvertretern, Behörden, Universitäten, Standardisierungs- und Zulassungsgremien sowie mit Firmen, die selbst an automatisierten Fahrsystemen oder deren Komponenten arbeiteten und immer noch arbeiten.

Aufgrund der erheblichen internationalen / weltweiten Resonanz der PEGASUS-Methodik [36], wurde im Dialog zwischen der VDA Leitinitiative und dem BMWK beschlossen, den PEGASUS-Staffelstab in größerem Rahmen weiterzutragen und in zwei Nachfolgeprojekten zu verankern, die eine Projektfamilie PEGASUS bilden: SetLevel, das sich mit der Weiterentwicklung von Simulationskomponenten (wie z.B. Sensormodellen), simulativen Plattformen und Werkzeugketten beschäftigen und das Projekt VVM, das sich auf die allgemeine Methodik der szenariobasierten Validierung und Verifikation konzentrieren und die Ergebnisse des SetLevel-Projektes nutzen sollte.

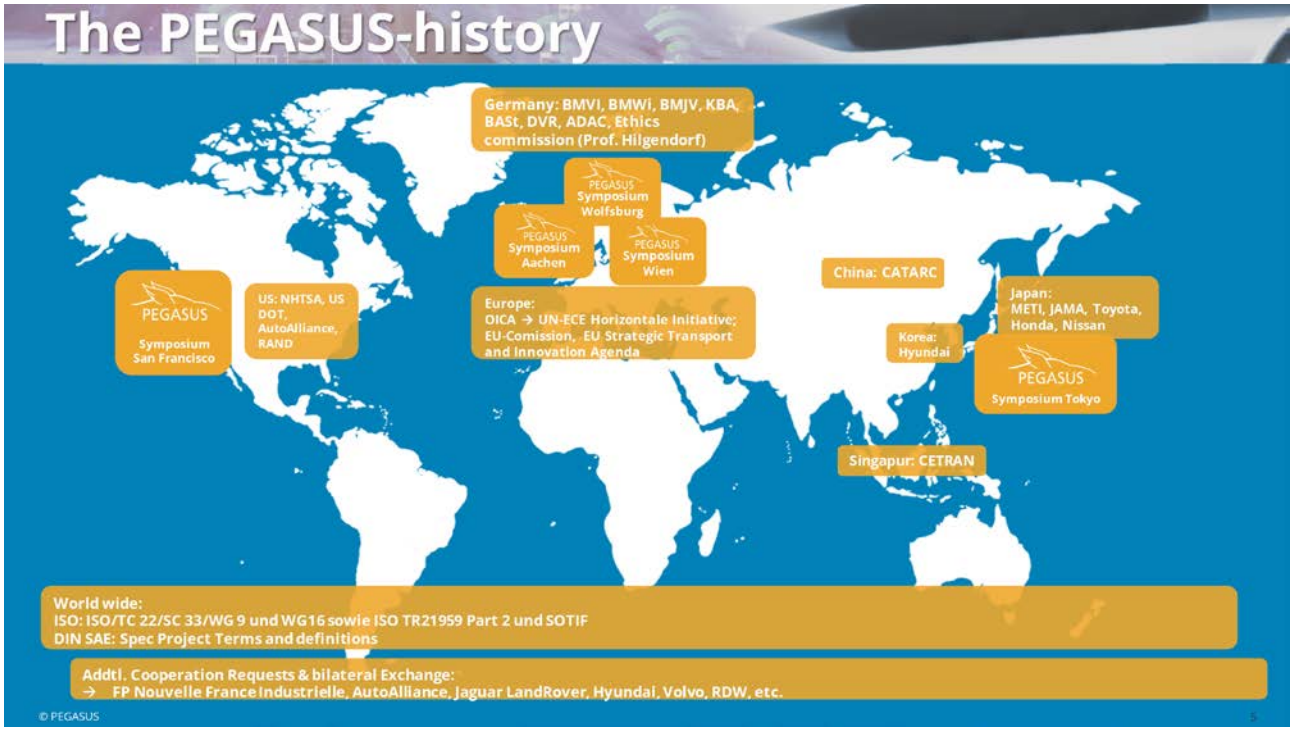


Abbildung 18: Überblick über die internationalen Aktivitäten von PEGASUS [35]

Ebenfalls von Anfang an war es PEGASUS wichtig Standards zu setzen und diese Standards in Hände zu geben, die sie auch nach dem Projektende weiter am Leben erhalten. Bei den in PEGASUS integrierten und adaptierten Sprachen und Interfaces handelte es sich um OpenDrive, OpenCRG, OpenScenario und OSI (OpenSimulationInterface). Diese wurden an ASAM mit der Auflage des freien Zugangs sowie der weiteren Pflege gegeben. ASAM entwickelte daraus in Kooperation mit den (ehemaligen) Projektpartnern nach Projektende die OpenX Familie [43] (siehe Abbildung 19).

Abbildung 19: PEGASUS-Transfer: Die OpenX Standards bei ASAM [43]

Weitere Aktivitäten sind aus der Abbildung 18 zu entnehmen. Herauszuheben sind der Multipillar Ansatz in den UN-ECE-Regularien [39], der SAE/ISO Standard zum szenariobasierten Testen und viele andere mehr.

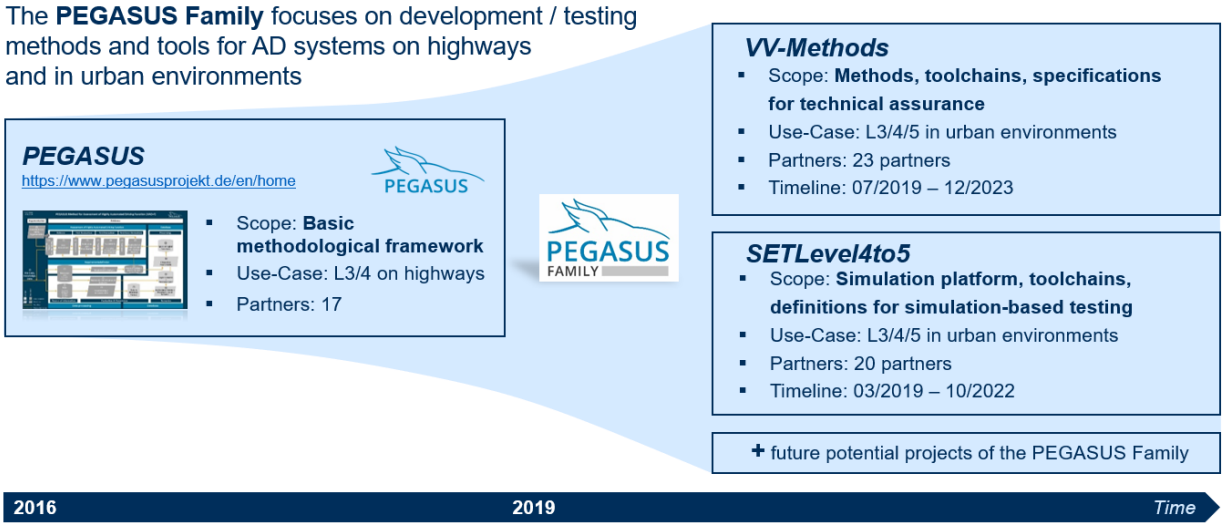


Abbildung 20: Hintergründe der PEGASUS-Projektfamilie

3.1.1.1.2 Kernergebnisse und gemeinsame Grundlagen

VVM erweiterte für seine Arbeiten die in PEGASUS betrachtete ODD “Autobahn” und “urbane Gebiete” (mit Autobahnen) und wählte eine SAE-Level 4 Kundenfunktion (siehe Kapitel 3.1.1.3) zur weiterführenden Systematisierung der PEGASUS-Methode. Wegen der komplexeren ODD entwickelte das VVM-Projekt neue Testverfahren, sowie Verbesserungen existierender, und lieferte einen Rahmen und Methoden für die Sicherheitsüberprüfung von automatisierten Fahrzeugen. Im Mittelpunkt der Projektarbeit waren der Anwendungsfall einer automatisierten Fahrfunktionen des SAE-Levels >= 3 im urbanen Kontext inklusive Stadtautobahn. Exemplarisch

wurde dafür die Kundenfunktion eines *urbanen Ruftaxis* (siehe Kapitel 3.1.1.3) betrachtet. Sie wurde nur exemplarisch in der Simulation jedoch nicht in projekteigenen Fahrzeugen dargestellt. Dies war nicht im Projektfokus.

Das VVM-Projekt baute dabei auf den Ergebnissen des ursprünglichen PEGASUS-Projekts auf, das sich als Fokus mit der Identifizierung und Beschreibung von kritischen Szenarien beispielhaft für ein ADS der SAE-Level 3 am Beispiel des Autobahnpiloten befasste. VVM erweiterte die PEGASUS-Methode auf Systeme des SAE-Level 4 mit dem Fokus auf neuen Herausforderungen im innerstädtischen Verkehr.

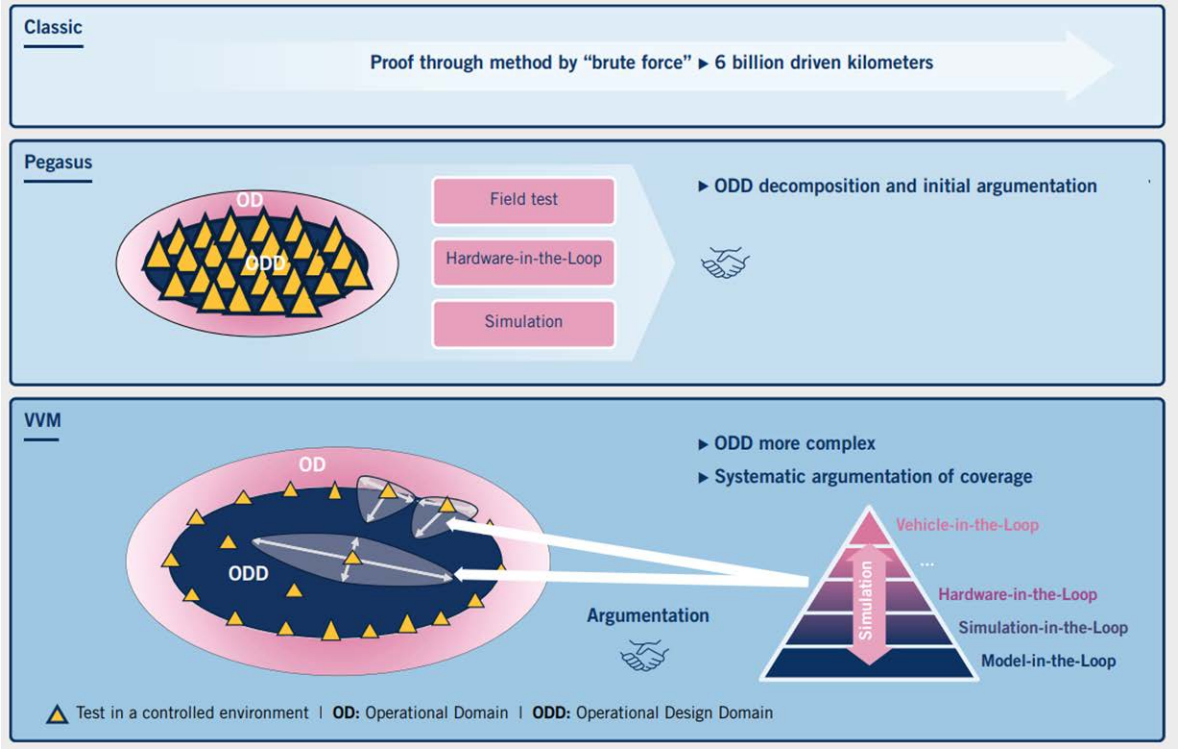


Abbildung 21: PEGASUS Ansatz im Vergleich zu den VVM-Erweiterungen

VVM arbeitete als Nachfolgeprojekt von PEGASUS auch an der Integration von Validierung und Verifizierung als einem integralen Bestandteil des Entwicklungsprozesses, um so eine nahtlose Argumentationskette für den Nachweis der Sicherheit und seine Machbarkeit zu demonstrieren. Alle möglichen Werkzeuge von Simulationen bis hin zu Testfahrten in der realen Welt werden so effizient wie möglich eingesetzt. Die klassische Variante der "Brute-Force"-Methoden zur Erprobung neuer Technologien stößt bei automatisierten Fahrsystemen in der Automobilindustrie an Grenzen, da die notwendigen Fahrstrecken nicht abdeckbar sind, besonders im Hinblick auf seltene Edge-Case-Szenarien (siehe auch [44]). Selbst existierende groß-dimensionierte Prototypflotten, die sich seit Jahren im internationalen Markt in Probebetrieb befinden, sind noch sehr weit von diesen Fahrleistungs-Dimensionen entfernt. Darum wurde schon im PEGASUS-Projekt, der szenariobasierte Ansatz vorgeschlagen. Aber auch hier trifft man aufgrund der Komplexität der Herausforderungen des automatisierten Fahrens in der Stadt auf ein analoges Problem, die sogenannte Parameter-Raum-Explosion: Aufgrund der Vielzahl der Parameter in möglichen Szenarien, die dem AD-System begegnen und der damit gekoppelten engen Abtastschritte würde dieses Phänomen zu einer hohen Anzahl an notwendigen Testszenarien führen würde. (siehe [45]). Daher wird der ursprüngliche PEGASUS-Ansatz via VVM um eine starke ausgebaute "Argumentation" konzeptionell erweitert. Zur Strukturierung des Bereichs der

Operational Domain und respektive der Operational Design Domain wird mit kleineren Basiselementen gearbeitet, die zu größeren Betriebsbereichen zusammengesetzt werden können. Zur Beschreibung des OD/ODD findet besonders das VVM 6-Ebenen-Modell [46] mit CORE-Szenarien zur strukturierten Modellierung der ODD seine Anwendung.

Um die VVM-Methode zu strukturieren, werden verschiedene Perspektiven wie

- “Development & Operation I Global” - also eine strukturierte Betrachtung von Entwicklungszeit und Systembetrieb, als allgemeine Prozessabbildung - “Global”
- “Development & Operation I Scenarios” - eine strukturierte Einbettung in das V-Modell mit Fokus auf Szenarien und szenarienorientierte Prozesserweiterung - “Scenarios”
- “Risk Management” - die konsequente Durchführung strukturierter Sicherheitsanalysen und Risikobewertungen,
- “Argumentation”, - die strukturierte Zusammenfügung der durch die VVM Methode erzeugten Evidenzen zu einer GSN-basierten Argumentation eines vom ADS beim Betrieb ausgehenden “akzeptablen Risikos”

Abbildung 22: Oberste Ebene der relevanten Perspektiven

sowie die Ebenen “Capablity-, Engineering-, Real-World-Layer” (zusammen ein Modell zur strukturierten Ableitung von Anforderungen und zur Gestaltung der Architektur jeweils für das ADS und die V&V Aktivitäten) betrachtet.

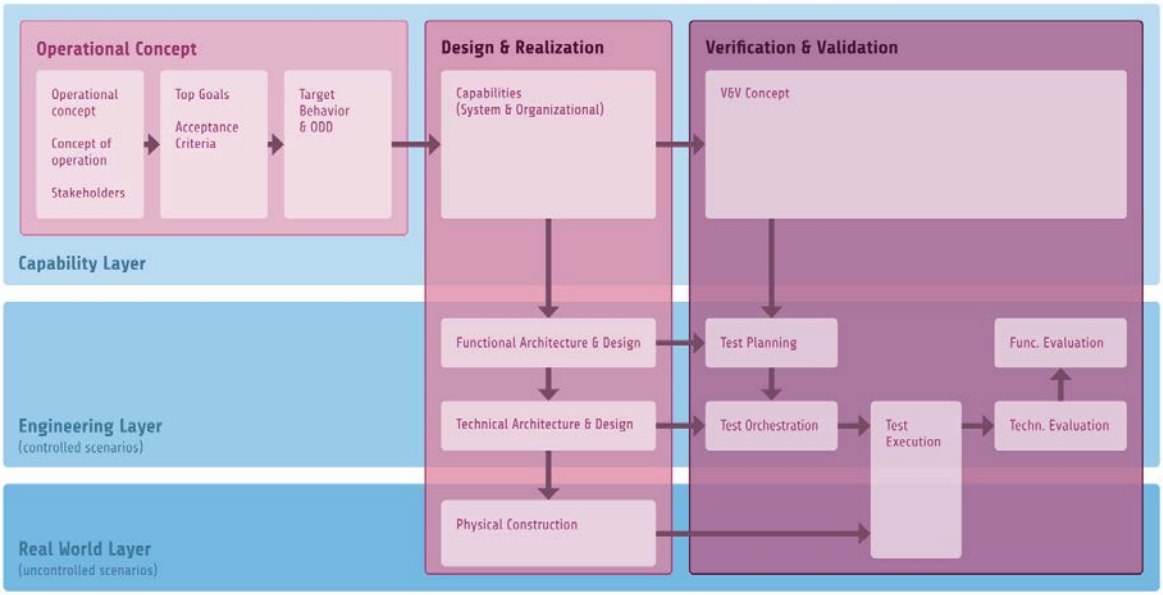


Abbildung 23: Capability, Engineering- und Real-World-Layer der VVM-Methode

Dabei geht VVM über den Rahmen des ursprünglichen PEGASUS-Projekts weit hinaus, passt das Original- PEGASUS 6-Layer-Modell für den urbanen Anwendungsfall an und setzt sein ODD-Metamodell auf diesen Grundlagen auf. Zusätzlich zu PEGASUS werden bei VVM auch die szenariobasierte Verhaltenspezifikation des AD-Systems, sowie die szenariobasierte Validation und Verifikation sowie die szenariobasierte Risikoevaluation in die Methode aufgenommen. Außerdem wurden die entsprechenden experimentellen Testmethoden und deren Zusammenspiel von reiner Simulation über Hardware-in-the-Loop und Vehicle-/Prototype-in-the-Loop-Methoden hin zu Prüfgelände- und Realwelttests verfeinert. Zudem wurden Ansätze entwickelt, um die Kluft zwischen simulativer Erprobung mit synthetischen Daten und aufgezeichneten Realwelttrajektorien adaptiv zu überbrücken.

Zusammengefasst lässt sich feststellen, dass die ursprüngliche PEGASUS-Methode, die sich weitgehend mit der rechten Seite des V-Modells beschäftigt hat, als PEGASUS VVM-Methode nun für den urbanen Anwendungsfall als Erweiterung sowohl die rechte wie die linke Seite des “V” mit szenariobasierten Methoden umfasst.

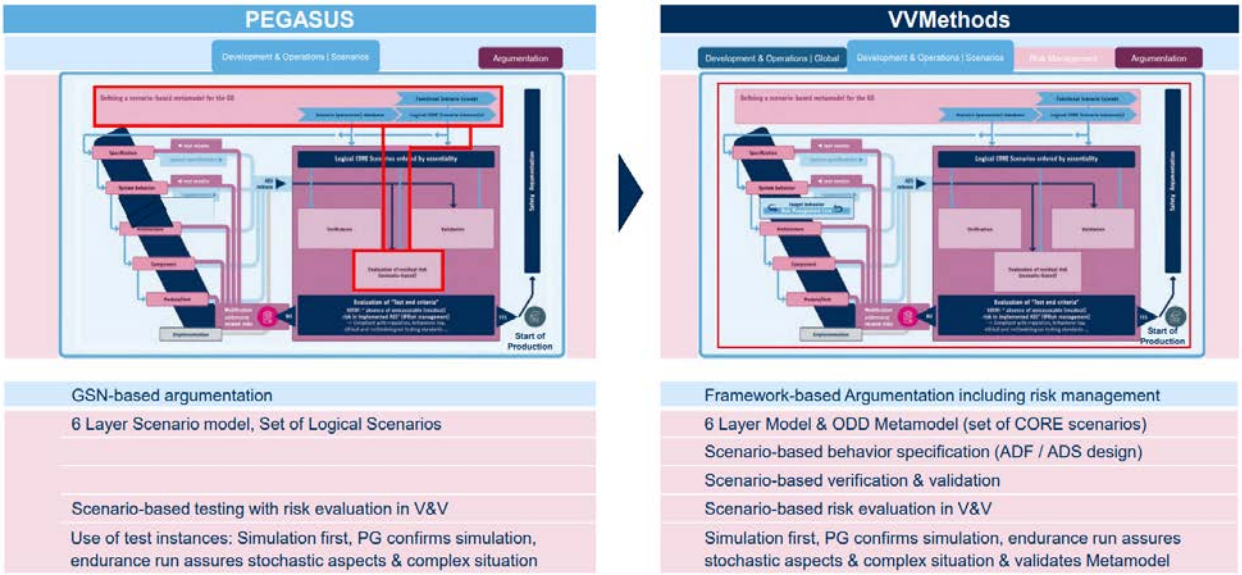


Abbildung 24: Vergleich PEGASUS vs. VVM-Gesamtmethode (siehe auch 3.1.1.2)

3.1.1.1.3 Standardisierung

Zahlreiche weltweit agierende Standardisierungsorganisationen, Gremien und Behörden sowie zusätzlich private Initiativen und Forschungsprojekte definieren technologische Elemente und Prozessschritte des virtuell geführten Sicherheitsnachweises für Automatische Fahrfunktionen. Dabei stehen neben den Prozessen auch Architekturen, Spezifikationen und Umsetzungspfade für die hochkomplexen Elemente des szenarienbasierten Sicherheitsnachweises im Fokus welche anwendungsnah und über viele Akteure reichende hinweg die nötigen Spezifikationen und Prozessschritte definieren, anhand derer konsistent und rückführbar der Nachweis geführt werden kann.

Als grundlegende Ausrichtung wurden hier zu Projektbeginn die wesentlichen existierenden sowie in Ausarbeitung befindlichen Dokumente v.a. von ISO, SAE, BSI, IEEE und ASAM gesichtet und die Relation der dortigen wesentlichen Definitionen in die Entwicklung der VVM-Gesamtmethode mit integriert sowie entsprechende Beteiligungen angestrebt und erzielt.

Zusätzlich zu dem methoden-, szenarien- und datengetriebenen Sicherheitsnachweis wie er durch Projekte wie VVMethoden und SET Level vorangetrieben wird liegt mit den regulatorischen Vorgaben aus den nationalen Gesetzgebungen in Deutschland (06/2022: https://www.gesetze-im-internet.de/afgbv/AFGBV.pdf) und Europa (08/2022: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1426) erstmalig ein verbindlicher Gesetzesrahmen vor, gegen den sich die Methodiken zum szenarienbasierten Sicherheitsnachweis messen lassen müssen.

Aus diesen Gründen strebte VVMethoden an, im Rahmen seiner Austausch- und Verbreitungsaktivitäten einen systematischen Austausch mit wesentlichen Standardisierungsorganisationen für die VVM Projektergebnisse zu schaffen, die VVM-Positionen in den Normen und Standards zu manifestieren und auch um dort wo geboten, die VVM-Gesamtmethode konform zu den aktuellen oder kommenden Standard- und Regelwerken auszurichten.

Bei den für VVMethoden relevanten Normen- und Standardisierungsaktivitäten standen insbesondere die folgenden Gruppierungen im Fokus von VVM und waren sowohl Impulsgeber und Spezifikationsbasis als teilweise auch Gegenstand der VVM Liaison Aktivitäten.

- ISO TC 22 SC 33 WG 9, dabei
    - Die WG 9 34501 - 34505 Familie, insbesondere 34502 - “"Engineering Framework and process of scenario-based evaluation“
    - sowie die angekündigte ISO WG 9 34505 “Evaluation of test scenarios for AD systems“
- ISO TC 22 SC 32 WG 13 TR 5083 “Road Vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation methods”
- ASAM Open.X Familie mit
    - OpenScenario
    - OpenSimInterface
    - OpenDRIVE
    - OpenXOntology
    - OpenODD
    - OpenLabel
    - OpenCRG
- UN ECE WP29 Gruppen VMAD, GRVA und GRVA

Ergänzend dazu lagen als Basiswerke die ISO 26262 (“Road vehicles – Functional safety“) und ISO 21448:2022 (“Road vehicles — Safety of the intended functionality“) zugrunde, diverse SAE Normen aus der SAE J30X Familie sowie SAE ORAD, die Safety Principles der Automated Vehicle Safety Consortiums (SAE AVSC) sowie die BS PAS Werke, z.B. 1883.

In Abbildung 25 sind wesentliche fachliche Verbindungen aufgezeigt zu konkreten Standardisierungen in denen VVM eine Wirkung erzielt hat.

Abbildung 25 - Fachliche Verbindungen VVM - ISO und UN ECE WP29

Abbildung 26: Übersicht über unterschiedlichen Aktivitäten auf den Gebieten Regulierung, Standardisierung, Forschungsprojekte und Datenmarktplätze.

Auswirkungen

- Austausch zwischen führenden Standardisierungsinitiativen und VVM während der gesamten Projektlaufzeit

Laufzeit

- VVM Sicherheitsargumentation, Risikomanagement, Kritikalitätsanalyse und Omega-Format in der Normung

Verbindungen zu externen Projekten

Während der Laufzeit des Projekts fand ein internationaler Austausch mit Initiativen zum szenariobasierten Testen unter dem Dach der PEGASUS-Projektfamilie gepflegt Projektfamilie statt, um

- sicherzustellen, dass der Sicherheitsfall, wie er von VVM definiert wurde interoperabel und austauschbar ist.
- gegenseitige Lieferketten zur Bereitstellung von Daten aufzubauen, inklusive Szenarien und Modelle für den Sicherheitsnachweis.
- gemeinsame zukünftige Aktivitäten zu definieren, die die VVM Methoden mit externen Daten- und Szenarioanbietern harmonisieren und zur Anwendung des Sicherheitsnachweises an Einsatzorten.

3.1.1.1.4 Fachsprache

Als Grundlage für die VVM-Methodik wurde eine VVM-projektübergreifende gemeinsame Fachsprache erstellt, aufbauend auf dem Glossar des ursprünglichen PEGASUS-Projekts [47]. Teil des Aufbaus der gemeinsamen Fachsprache ist die Identifikation, Erfassung und Bewertung potentieller Fachtermini. Diese Begriffe wurden in einer Sammlung katalogisiert um anschließend im Projekt analysiert zu werden. Ausgang dieses Vorgangs ist eine Sammlung von Begriffen zur Schaffung eines gemeinsamen Verständnisses der ADAS/ADS – Gemeinschaft. Der Zugriff auf die Sammlung abgestimmter Terme wurde in einem multimodalen Ansatz zur Darstellung realisiert. Basis dieser Darstellung ist ein vollständiger, verständlicher Präsentationsansatz, aus welchem ein Dokument sowie ein Webdokument resultiert. Neben der internen, VVM-weiten Abstimmung der gemeinsamen Fachsprache, wurde im Sinne der zentralen Bedeutung der Verbindung zu externen Projekten eine VVM übergreifende Kooperation durchgeführt. Ziel dieser Kooperation mit Projekten wie SetLevel, Vivid/Vivaldi und Gaia-X war die Abstimmung identifizierter Begriffe, welche bereits einen projektinternen Konsens erzielt haben, auch im deutschen ADAS/ADS-Ökosystem zu synchronisieren. Zusammenfassend sollten folgende Ziele erreicht werden:

- Erstellung einer Sammlung abgestimmter Fachbegriffe entscheidend für das gemeinsame Verständnis der ADAS/AD-Gemeinschaft.
- Erstellung eines lebendigen Dokuments: Multimodale Darstellung - verständlich, vollständig, koordiniert.
- Abstimmung mit deutschen ADAS/AD-Ökosystem Projekten zu einer gemeinsamen "Fachsprache", u.a. SetLevel, Vivid/Vivaldi und Gaia-X.

Die Methode zur Abstimmung nahm sich zwei zentralen Herausforderungen an. Zum einen stand die Frage nach einem Ansatz zur kooperativen Arbeit um wichtige Begriffe zu definieren und identifizieren. Das Ergebnis dieses Ansatzes ist eine Sammlung von Fachtermini, ein Glossar. Hieraus folgte die nächste Herausforderung: Wie kann dieses Glossar präsentiert werden, sodass auch Personen außerhalb des Projekts darauf zugreifen und es verstehen können.

Hierzu wurden Konsultationen zur Identifizierung und Definition von mehr als 100 Fachbegriffen durchgeführt. Im Rahmen der Erarbeitung und Abstimmung einer einheitlichen Fachsprache in den Projekten der PEGASUS-Familie, wurden überblicksartig folgende drei Aktivitäten angewendet.

(1) Der **Ansatz zur ersten Herausforderung**, der Identifikation und Definition von Begriffen, wurden projektinterne Konsultationen sowie projektübergreifende Abstimmungen durchgeführt. Während der Konsultation wurden mehr als 100 Fachbegriffe abgestimmt, die für das allgemeine VVM-Verständnis wichtig sind. Zum besseren Verständnis des Kontexts von Fachbegriffen, sowie der verbesserten Suche und Katalogisierung wurden den Begriffen zusätzlich zur Definition

Metainformationen hinzugefügt. Diese Metainformationen bestehen aus der Intention, welche hinter dem Begriff steht.

Das Feld Intention wird durch eine Auswahl von Begriffen, einer Intentionskategorie, befüllt. Diese Kategorien richten sich nach der Frage, was dieser Begriff beschreibt.

- Die Kategorie „Benennen“ wird gewählt, wenn der Begriff eine Gegebenheit beschreibt.
- „Beschreiben“ wird verwendet, wenn durch den Begriff ein Geschehen beschrieben werden kann.
- „Bemessen“ wird gewählt, wenn der Begriff relevante Parameter, zum Beispiel eines Verkehrsszenarios“ bezeichnet.
- „Vergleichen“ wird gewählt, falls der Begriff eine Beziehung zwischen ähnlichen Entitäten herstellt.
- Letztlich wird „Beurteilen“ verwendet, wenn ein Begriff Elemente wie Gesetze und Metriken anwendet, um Vorgänge zu klassifizieren.

Metainformationen ist die detaillierte Intention. Die detaillierte Intention erweitert die Intentionskategorie um eine Erläuterung, was mit dem Begriff gemacht wird. Neben der Intention werden in den Metainformationen auch verwandte Objekte/Subjekte erfasst, sowie der Adressat. Bei näherer Verwandtschaft zu anderen Begriffen wird die Metainformation „Relation zu anderen Begriffen“ mit diesen Begriffen befüllt. Hierdurch ist eine Navigation zwischen verwandten Begriffen möglich. Gleichzeitig können Begriffe, welche klar von dem betroffenen Term zu unterscheiden sind, in der Metainformation „Abgrenzung zu“ hinterlegt werden.

(2) Der **Ansatz zur zweiten Herausforderung** wurde durch das Anbieten einer Darstellung in der Form eines modernen Webdokuments realisiert. Durch dieses Webdokument ist eine Suche nach Begriffen möglich. Die Suche kann über eine Suchleiste sowie über eine sortierte Liste der Begriffe durchgeführt werden. Die Begriffsbeschreibungen selbst stellen neben dem Begriff sowie der Erläuterung auch die Metainformation dar. Begriffe der Erläuterung sowie Begriffe der Metainformationen können als Link aufgerufen, oder direkt auf der Seite des enthaltenden Begriffs dargestellt werden. Dies ermöglicht eine einfache Navigation durch einen Themenkomplex. Das Webdokument ist unter folgendem Link erreichbar:
https://zenodo.org/records/10533077

(3) Die intern abgestimmten Begriffe wurden VVM-übergreifend mit Partnern der PEGASUS-Familie und darüber hinaus abgestimmt. Diese projekt-externen Partner setzten sich aus Gaia-X, Vivid/Vivaldi und SetLevel zusammen. Aus dieser Partnerschaft ist ein weiteres Glossar entstanden für einen **übergreifenden Austausch innerhalb des deutschen ADAS/AD-Ökosystem und deren internationalen Partner**.

Das gemeinsame übergeordnete Glossar der PEGASUS-Familie kann unter folgendem Link erreicht werden Glossary - VIVID German-Japan joint virtual validation methodology for intelligent driving systems (safecad-vivid.net).

3.1.1.2 Methodischer Überblick

In diesem Kapitel wird die VVM-Gesamtmethode auf einer hohen Abstraktionsebene beschrieben. Die erfolgt unter den Gesichtspunkten: methodisches Vorgehen, Sicherheitsargumentation,

gesellschaftliche Erwartung und Erfüllung der Sicherheit, Konzept für die Absicherung des Sicherheitsanspruches, Herausforderung Sicherheit-Management automatisierter Fahrsysteme, Strategischer Link zwischen Test & Absicherung und der Sicherheitsargumentation, Traceability und Durchgängigkeit. In den Kapitel 3.1.1.3 bis 3.1.1.9 wird auf Details eingegangen.

VVM-Gesamtmethode - eine szenariobasierte Methodik für die Entwicklung eines automatisierten Fahrsystems

In der Automobilentwicklung ist das V-Modell eine etablierte Methodik zur Beschreibung des Entwicklungsprozesses. Vorteile des V-Modells sind: ein strukturiertes Top-Down Vorgehen, klare Verbindung von Anforderungen und Tests, Nachvollziehbarkeit und Dokumentation. Die Phasen der Systementwicklung sind: Entwurf, Implementierung und Validierung&Verifikation (V&V). In den Entwurfsphasen des V-Modells wird das (mechatronische) Fahrzeugsystem - hier ein automatisches Fahrsystem (ADS) - entworfen und immer detaillierter beschrieben. Die Schritte laufen als Top-Bottom-Prinzip ab. Die Entwicklungsphase ist geprägt von Anforderungsanalyse, Systemdesign, Systemarchitektur und Komponentenentwurf. Die Implementierung ist die eigentliche Realisierung des ADS. Im letzten Schritt, der Absicherung, finden zu jeder Entwurfsphase verschiedene Testphasen statt. Die Tests finden im Bottom-Up-Prinzip statt. Es werden zuerst die Komponentenphase getestet, bis im Abnahmetest das gesamte System geprüft wird. Die Schritte sind: Unit- und Komponententests, Integrationstests, Systemtests und die Systemvalidierung.

Normen, wie etwa die ISO 26262 [8], ISO 21448 [48] sowie Standards wie etwa ISO 3450x, ISO/CD TS 5083, ISO/SAE CD 21434 sowie der ständig fortgeschriebene Stand-der-Technik beschreiben Anforderungen an die Ausgestaltung des Prozesses sowie der tieferen Prozessebenen. Das V-Modell selbst ist ein Teil des Qualitätsmanagements im Entwicklungsprozess der Automobilindustrie, daher wird es in diesem Kontext zur Beschreibung der VVM Methode verwendet. Es ist ein seit Jahrzehnten etablierter Prozess in der Automobilindustrie.

Auf der Grundlage des V-Modells definiert die Norm ISO 26262 [8] ein Verfahren zur Gewährleistung der funktionalen Sicherheit von Systemen in ihrer Entwicklung vor deren Inbetriebnahme. Die Abschnitte 3 (Konzeptphase) bis 7 (Produktion und Betrieb) in der Norm sind an dem V-Modell ausgerichtet. Die Kernidee des V-Modells ist die Beschreibung des Gesamtprozesses durch eine Folge von logischen (Sub-) Prozessen. Standards wie etwa SPICE schlagen Detaillierungen vor, folgen aber dem Model des Entwicklungsprozesses. Eine Darstellungsform der VVM-Gesamtmethode ist daher das V-Modell und notwendige Ergänzungen. (siehe Abbildung 39)

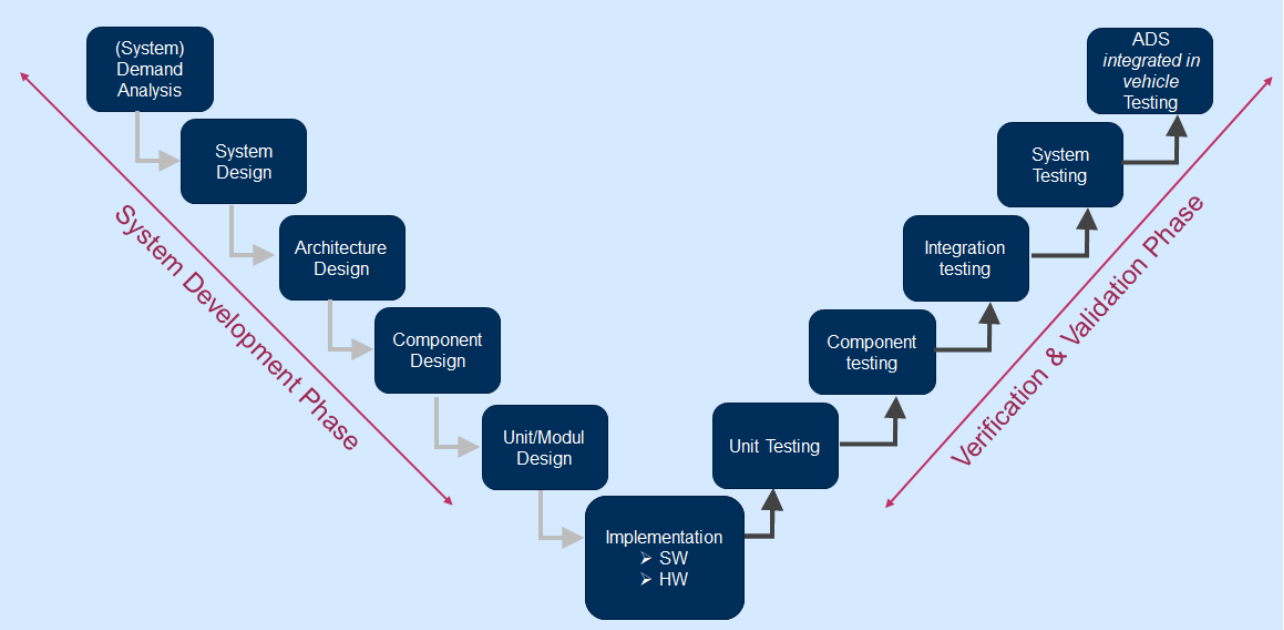


Abbildung 27: V-Modell (Prozessmodell) nach VDI-Entwicklungsmethodik für mechatronische Systeme 2004

Die Leistung des Vorgänger-Projektes PEGASUS [36] war es, die Rolle der Simulation bei den Herstellern von automatisierten Fahrsystemen durch szenariobasiertes Testen zu verankern. Die Integration des Gesamtsystems und die Integration des ADS in das Fahrzeug werden inzwischen insbesondere mit digitalen Plattformen auf der Basis von Simulationsmethoden verifiziert. (siehe Kapitel 3.1.1.2). Das Spektrum der eingesetzten Test-Instanzen reicht von Model-in-the-Loop, Code-in-the-Loop, Hardware-in-the-Loop, (single and cluster), vehicle-in-the-Loop bis Human-in-the-Loop. Die aus den Simulationen gewonnenen Erkenntnisse werden durch abgestimmte Erprobungen auf Testgeländen -etwa durch detailliert mit vorherigen Simulationen synchronisierten Tests mit Realfahrzeugen, Soft-Crash-Targets und Dummies - sowie im realen Fahrbetrieb validiert. Ein ausgeklügeltes Validierungs- und Verifikationskonzept strukturiert die Testziele, die zur Freigabe notwendig sind, sowie die zu verwendenden Methoden zu Ihrer Erbringung und beschreibt, wie sie auf die unterschiedlichen Testinstanzen verteilt werden, damit am Ende nur noch wenige Tests mit Realfahrzeugen notwendig sind.

VVM erweitert diesen Ansatz zu einer ganzheitlichen Betrachtung des Entwicklungsprozesses, der eine strukturierte Argumentation dafür liefert, dass das ADS ein sicheres Verhalten auf einem akzeptablen Niveau des Restrisikos für alle Bedingungen erreicht, die den spezifizierten Betriebsbedingungen und -zuständen entsprechen, die die Zielanwendungsdomäne beschreiben. Im Rahmen der hier dargestellten VVM-Gesamtmethode werden exemplarisch sicherheitsrelevante (Teil) Ziele so ausgewählt, dass ein sicheres, konformes Verhalten des ADS in seiner ODD argumentiert werden kann. Abbildung 28 zeigt die beispielhafte Zerlegung des Ziels “akzeptables Risiko” in die sicherheitsrelevanten (Teil-) Ziele “Funktionale Sicherheit”, die „Sicherheit des Systemverhaltens“ (SOTIF), die „Konformität mit Gesetzen und Vorschriften sowie mit gesellschaftlichen / ethische Anforderungen“, wie sie sich z.B. aus ethischen Diskussionen über die Höhe des akzeptablen Risikos ergeben. VVM erweitert das bisherige "szenariobasierte Testen" zu einem "argumentations- und szenariobasierten Entwickeln". Kernelemente des erweiterten VVM-Ansatzes sind:

- **Integration der Sicherheitsargumentation** in das Design der Entwicklung und Absicherung der ADS durch frühzeitige Abstimmung der Artefakte sowie ihrer prozessualen und methodischen Anforderungen an ihre Generierung im Rahmen der Entwicklung, so dass sie konzeptionell in die Phasen der Systementwicklung, der Implementierung sowie der Verifikation und Validierung einfließen können. (argumentative V&V). (siehe hierzu: Kapitel 3.1.1.2 Methodischer Überblick, Kapitel 3.1.1.2.1 Sicherheitsargumentation)
- **Integration eines durchgängigen Risikomanagements** (Kapitel 3.1.1.2.5) im Rahmen der Anforderungsanalyse, Spezifikation, dem Design eines sicheren und konformen Systemverhaltens sowie der Architektur des ADS und ferner bei dessen Absicherung (in der Verifikation & Validierungsphase). Eine Folge daraus ist, die durchgängige Verwendung gleicher Risikomodelle, Evaluierungsfunktionen und Risikoakzeptanzlevel im Entwicklungsprozess (V-Modell).
- **Integration des ODD-Metamodell-Ansatzes** für die durchgängige Analyse der Betriebsdomäne (ODD), der Verhaltens- und Systemspezifikation sowie in der Verifikation und Validierung (siehe hierzu Kapitel 3.1.1.4 und 3.1.1.5 Szenarienabstraktion). Der ODD Metamodellansatz ist insbesondere die Voraussetzung für die Integration des safety-by-design Ansatzes, der die Entwicklung eines robusten und sicheren automatisierten Fahrsystems durch den szenariobasierten Entwurf des Systemverhaltens addressiert und die technologische Fähigkeit durch die Analyse von Anwendungsfällen und Szenarien gewährleitet.
- **Durchgängige Nutzung von Dekompositionsstrategien**, insbesondere im Systemdesign, der Verhaltensspezifikation, der Architektur sowie im Rahmen der Verifikation und Validierung, um den Aufwand zu minimieren. (siehe hierzu Kapitel 3.1.1.4 und 3.1.1.5 Szenarienabstraktion)

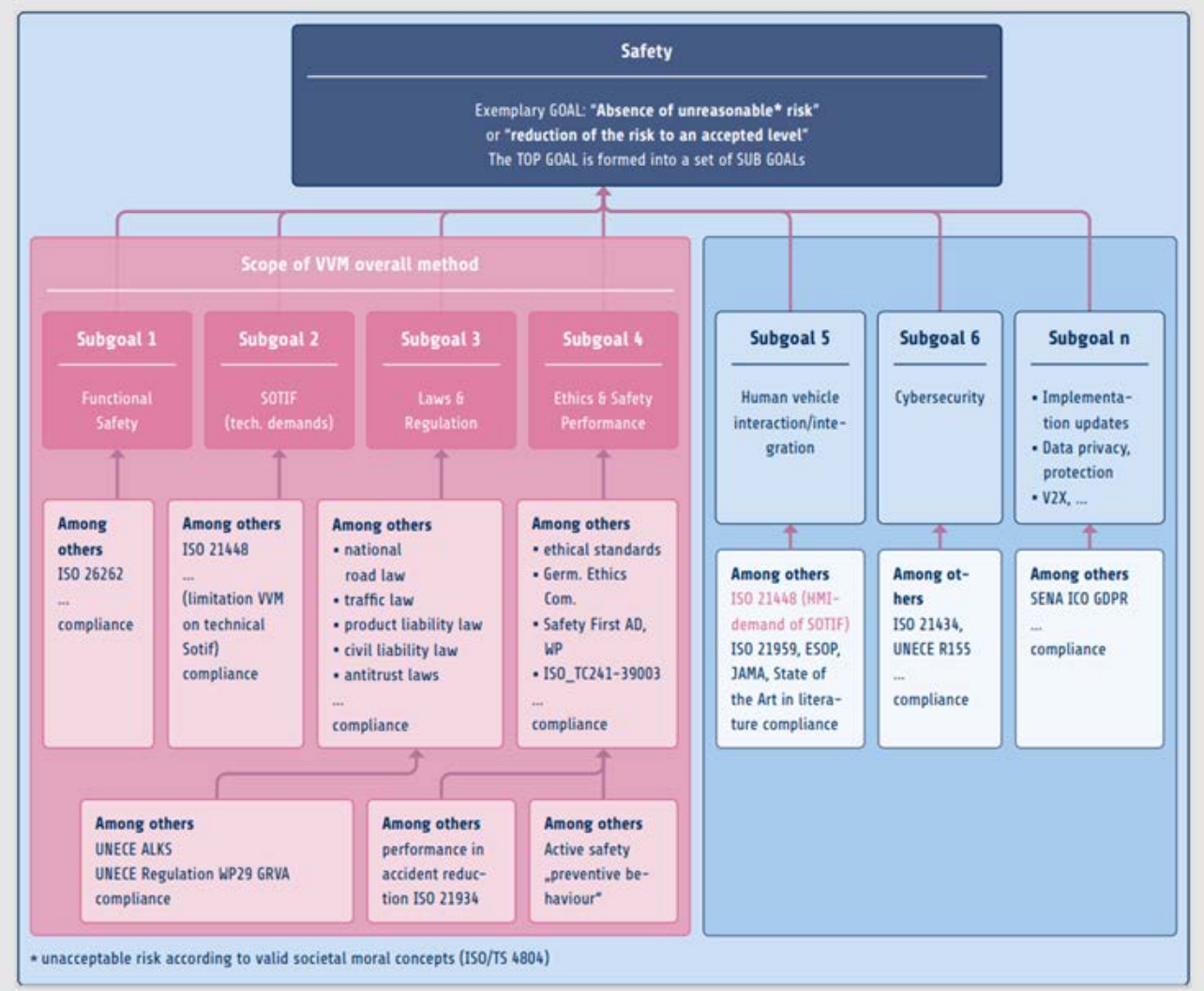


Abbildung 28: Beispielhafte Zerlegung des sicherheitsrelevanten (Argumentations- / Entwicklungs-) Ziels (“Top Goal”) “akzeptables Risiko” in (Teil-) Ziele (“Sub Goals”, Rot hinterlegt), wie sie im Rahmen der VVM-Gesamtmethode für die ADS Sicherheitsargumentation (ADS Safety Case) benutzt werden.

Der Bedarf an eine Dekompositionsfähigkeit des ADS entsteht einerseits aus der arbeitsteiligen Organisation bei der Entwicklung von Fahrzeugen und Fahrzeugsystemen intern und in Kooperationen sowie andererseits aus der Notwendigkeit der Beherrschbarkeit der Komplexität technischer Systeme im Rahmen ihrer technischen Entwicklung. Die Dekomposition des ADS resultiert einerseits aus unterschiedlichen, separablen Anforderungen sowie daraus entstandenen getrennt entwickel- bzw. testbaren Funktionalitäten, wie sie z.B. durch Zerlegung der Kundenfunktion in Teilfunktionen (wie z.B. in Gefahrenhandling) und Wirkketten, sowie im Bereich der Validierung und Verifikation Trennbarkeit der z.B. Testobjekte, der Testräume in Teilparameterräume, der Steuerung des Validierungsprozesses und Ermittlung des Restrisikos des ADS in Bezug auf Szenarioklassen. In der arbeitsteiligen, komplexen Projektstruktur und den daraus resultierenden internen sowie externen Zuliefern bzw. Beteiligten ist die Forderung nach Dekomposition nicht nur fachlich, sondern auch organisatorisch zwingend notwendig.

Daraus folgt die konsistente Anwendung eines ausreichend vollständigen Metamodells für die ODD und einer Szenariendatenbank als Werkzeug zur Bereitstellung von Expositionsdaten für

Szenarien und Szenarioparameter für das Systemdesign und den V&V-Prozess. Auf diese Weise werden die Anforderungen an das System vorstrukturiert und eine Verifikation durch die intelligente Gestaltung von Tests durch Integration von Simulationsstrategien mit Tests auf Versuchsgeländen sowie Erprobungen auf der Straße als integraler Bestandteil des Entwicklungsprozesses ermöglicht. Dies begünstigt auch ein KPI-Tool zur Strukturierung einer ganzheitlichen Validierung.

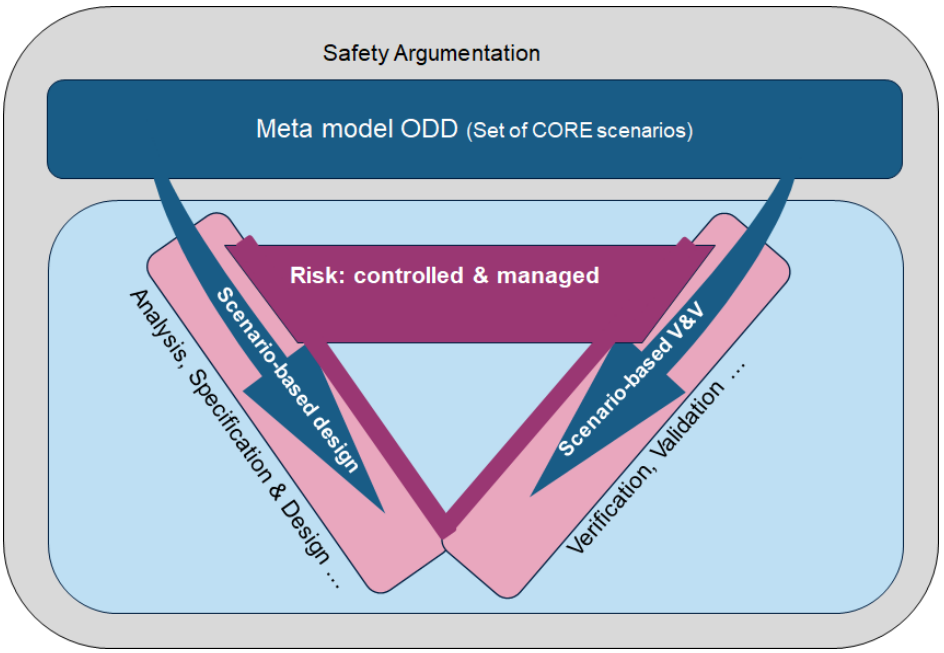


Abbildung 29: Die Basis-Struktur der VVM-Gesamtmethode

Das ODD-Metamodell liefert ein valides, ausreichend vollständiges und relevantes Bild der ODD. Die Verwendung des ODD-Metamodells gewährleistet konsistent eine repräsentative Problem-/Domänenanalyse, ein adäquates ADS-Design und eine adäquate Fahrzeugintegration sowie geeignete Nachweise aus dem erweiterten szenariobasierten Verifikations- und Validierungsprozess, wie in der allgemeinen VVM-Methode beschrieben. Im Folgenden wird gezeigt, wie es sich auf natürliche Weise in den Entwicklungsprozess eines Herstellers von automatisierten Fahrsystemen eingliedern lässt. (siehe Kapitel 3.1.1.4 Szenarienabstraktion Grundlagen)

Ziel und Geltungsbereich

Die VVM-Gesamtmethode liefert Evidenzen, die im Rahmen des ADS-Safety Cases eine strukturierte Argumentation stützen. Diese Argumentation belegt nachvollziehbar und stichhaltig, dass der Betrieb eines mit ADS ausgestatteten Fahrzeugs in seiner Zielbetriebsdomäne frei von unverhältnismäßigen Risiken für Fahrer, Beifahrer und andere Verkehrsteilnehmer ist.

Bei dem Fahrzeug handelt es sich um ein Straßenfahrzeug, das mit einem automatisierten Fahrsystem (Automated Driving System - ADS) nach SAE J 3016 ausgerüstet ist.

Die VVM-Gesamtmethode betrachtet ausschließlich die Elemente und ihre Dekomposition in Bezug auf die Entwicklung und V&V, die durch die Integration in eine funktionale Wirkkette einen besonderen Einfluss auf die Fahrautomation haben.

Die VVM-Gesamtmethode konzentriert sich darauf, die im Projekt PEGASUS entwickelte szenariobasierte Testmethodik für das Gesamtsystem weiterzuentwickeln. Das Ziel der Verifikation und Validierung besteht darin, den Entwicklungsstand (Release) hinsichtlich seiner Eignung für die Produktion bzw. einer Serienfreigabe zu bewerten.

Die VVM-Gesamtmethodik ist eine Zusammenstellung von methodischen Bausteinen zu einem Gesamtvorgehen, das die sicherheitstechnische Argumentation mit konkreten und belastbaren Nachweisen untermauert. Bewährte Einzelmethoden aus der Systementwicklung (linke Seite des V-Modells) und der Validierung/Verifikation (rechte Seite des V-Modells) werden hier zu einer umfassenden, in sich geschlossenen und konsistenten Methoden- und Ergebnisverknüpfung zusammengefasst.

Es werden insbesondere Aspekte adressiert, die sich aus dem Systemverhalten und der Architektur ergeben:

- Es wird eine fehlende Instanz des Fahrers integriert, d. h. eine Methode zur Bestimmung des Sollverhaltens für ein sicheres und regelkonformes Verhalten des automatisierten Fahrsystems mit einem akzeptablen Restrisiko für alle Bedingungen, die den spezifizierten Betriebsbedingungen und -zuständen entsprechen, die den Zielbetriebsbereich beschreiben.
- Es wird der Nachweis erbracht, dass das ADS in der Lage ist, Unfälle zu vermeiden oder deren Schwere zu vermindern, im Sinne einer Reduktion des Risikos und einer positiven Risiko-Bilanz mit Fahrerleistungsreferenz, also einer besseren Systemperformanz als beispielsweise der eines durchschnittlichen menschlichen Fahrers in dem konkreten Szenario. Dabei wird insbesondere die sichere Interaktion mit den anderen Verkehrsteilnehmern und der Umgebung betrachtet.
- Es wird die Wirksamkeit technischer Maßnahmen auf unterschiedlichen Betrachtungsebenen (Verkehrssystem, EGO Perspektive) eruiert.
- Es wird die Beherrschung einer sich ständig weiterentwickelnden und verändernden Umwelt (insbesondere des Umverkehrs, offener Kontext, lernendes System, …) bewertet.
- Es wird die Notwendigkeit der Ausfallsicherheit (Fail Operational Konzepte) bei der Auslegung der Architektur betrachtet.

Im Rahmen dieses Überblicks wird die VVM-Gesamtmethode auf System- und Integrationsebenen während der Entwicklung und Absicherung detailliert dargestellt. Eine grafische Darstellung ist in Abbildung 30 zu finden.

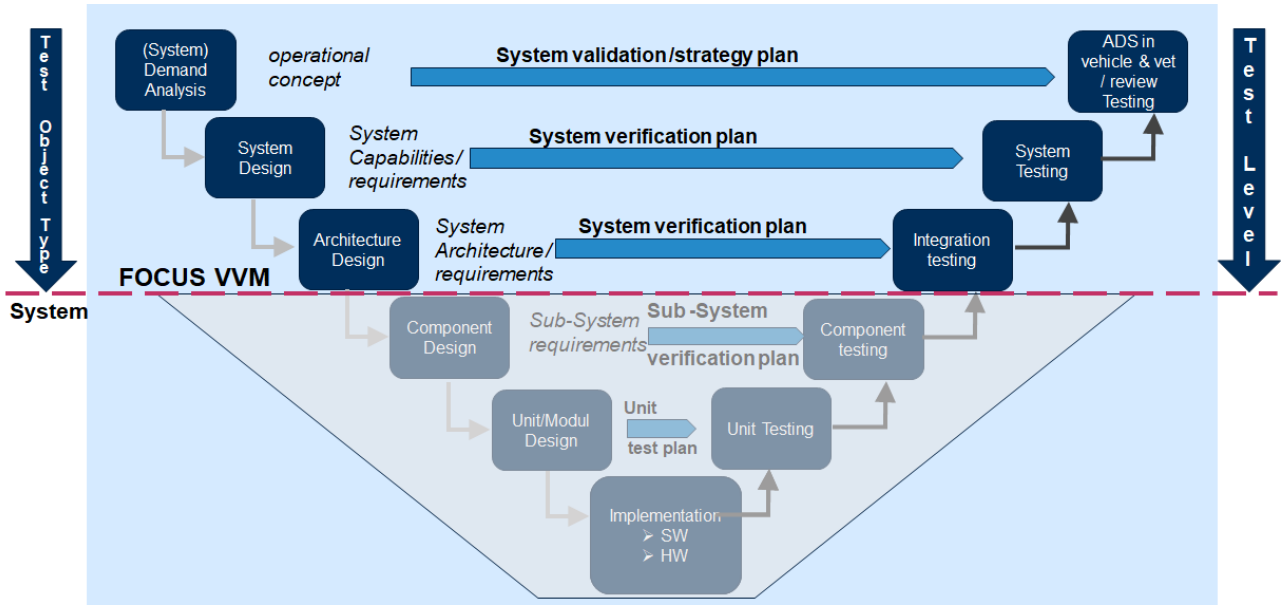


Abbildung 30: Beispielhaft gewählte Grenzen der Testtiefe (Integrations- bzw. Systemlevel) und Testobjekte, in den Darstellungen der VVM-Gesamtmethode.

Die methodische Vorgehensweise bei der strukturierten Argumentation und insbesondere der Verknüpfung der Evidenzen mit der überzeugend, nachvollziehbar und stichhaltig belegt wird, dass der Betrieb des mit ADS ausgestatteten Fahrzeugs in einer bestimmten Umgebung sicher ist, wird in diesem Kapitel dargelegt.

Im Folgenden sollen die (Kern-) Ergänzungen dargestellt werden, die aus Sicht VVM-Gesamtmethode in der Entwicklungs- sowie der Validierungs- und Verifikationsphase in einen durch das V-Modell (Abbildung 33) beschriebenen Entwicklungsprozess einzubinden sind.

Adventive Elemente für die Entwicklungsphase

Das **ODD-Metamodell** wird ergänzt um alle Teilschritte des V-Modells szenariobasiert durchlaufen zu können. Damit ist es möglich, die Entwicklungsphase, die Systemabsicherung und das Datamining auf Messdaten durchgängig mit denselben, die ODD valide repräsentierenden Szenarienklassen durchzuführen.

Die **OD-Domänen-Analyse** wird ergänzt, um ein detailliertes Verständnis von Stakeholderinteressen und zu erwartenden Betriebsbedingungen und -zuständen zu erlangen. Daraus können dann die sicherheitsrelevanten Fähigkeiten abgeleitet werden, die in der gewählten Betriebsumgebung etwa durch Designentscheidungen aufrechterhalten werden müssen.

Der **Risk Management Core** (RMC) wird ergänzt, da er einen Prozessrahmen für ein durchgängiges Risikomanagement bereitstellt. Im Rahmen der Spezifikation des Sollverhaltens des ADS ist der RMC ein Kernelement um argumentieren zu können, dass der Prozess der Spezifikation des Sollverhaltens des ADS eine risikobasierte Verhaltensspezifikation liefert, die die Anforderungen an die Verhaltenssicherheit einschließlich der erforderlichen Integrität enthält. Dies gilt insbesondere für die Spezifikation der Architektur und des Systemverhaltens im Umgang mit Gefahren und Auslösern für gefährliches oder unbeabsichtigtes Verhalten. Damit wird ein konsistenter und durchgängiger Umgang mit dem Risiko sowohl in der Phase der Entwicklung als auch in der Phase der Absicherung ermöglicht. Dies ermöglicht zudem die durchgängige

Verwendung von gleichen Risikomodellen, Evaluierungsfunktionen und Risikoakzeptanzlevel im gesamten Entwicklungsprozess (V-Modell).

ODD-Metamodell und die OD-Domänen-Analyse tragen zur Reduktion der Spezifizierungslücke und damit zur Reduktion der “unkown / unknown” bei. Der ODD Metamodellansatz in Kombination mit der OD-Domänen-Analyse bilden die Voraussetzung für die Integration des „safety-by-design“ Ansatzes, der die Entwicklung eines robusten und sicheren automatisierten Fahrsystems durch den szenariobasierten Entwurf des Systemverhaltens adressiert und die technologische Fähigkeit durch die Analyse von Anwendungsfällen und Szenarien gewährleistet. Der RMC schafft Transparenz indem er eine durchgängige Verwendung von gleichen Risikomodellen, Evaluierungsfunktionen und Risikoakzeptanzlevel im Entwicklungsprozess für die Spezifikation von Verhalten und Architektur sowie zur Bewertung des implementierten ADS ermöglicht. Dadurch wird die Reduktion des Unfallrisikos als Evaluationskriterium eines ADS Releases sowohl im Design als auch in der Phase der Verifikation und Validierung in die Entwicklungsphase integriert. Damit nähern sich auch die Modellwelten ISO 26262 (FUSA) und ISO 21448 (SOTIF) an.

Abbildung 31 zeigt eine modifizierte Darstellung des V-Modells aus Abbildung 33. Es wurden die zuvor definierten (Kern-) Elemente für die Entwicklungsphase eines ADS integriert.

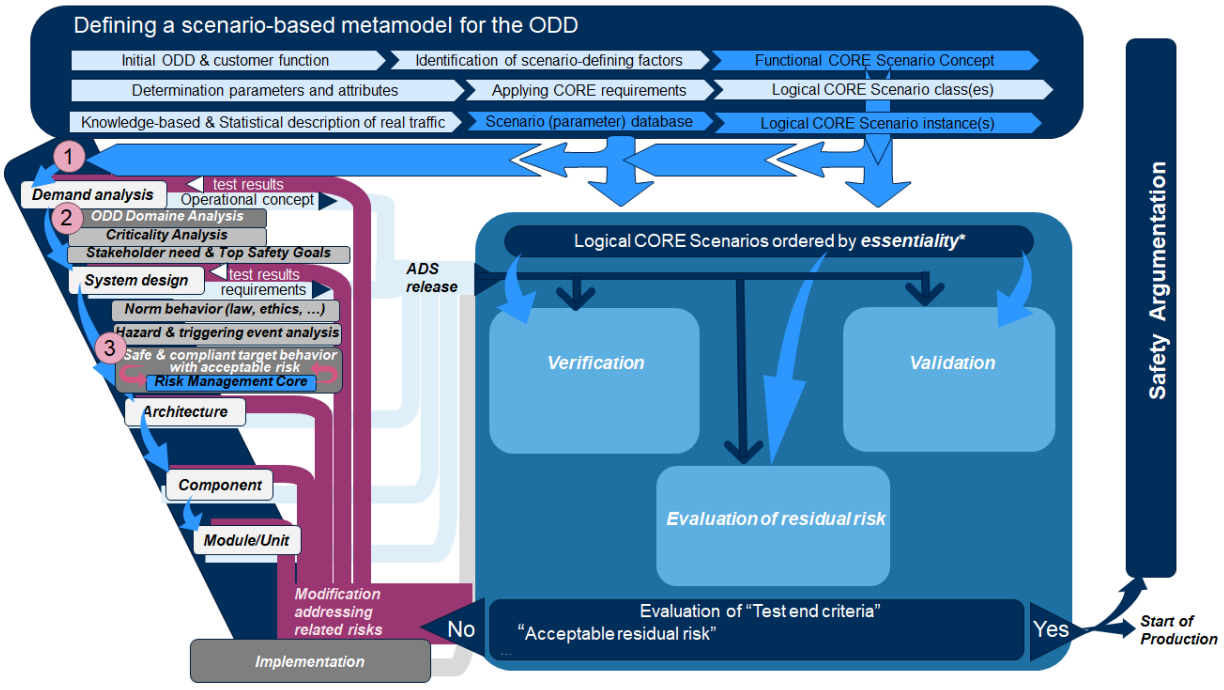


Abbildung 31: V-Modell (modifizierte Darstellung) mit den adventiven(Kern-) Elementen der VVM-Gesamtmethode in der Entwicklungsphase (linke Seite V-Modell)

One fits for all - ein szenariobasiertes Metamodell für die ODD, das durchgängig im gesamten Entwicklungsprozess eingesetzt wird.

Für die Umsetzung von szenariobasiertem Testen/Verifizieren in der Simulation sowie auf Testgeländen ist es notwendig, dass Anforderungen, die das Systemverhalten oder Grenzwerte für die Systemperformance definieren, in Parameterräumen mit Sampling-Methoden überprüft und bewertet werden können. Voraussetzung hierfür ist ein durchgängig nutzbares, strukturiertes Modell der ODD.

In PEGASUS wurde die Szenariobeschreibung in Form des 6-Ebenen-Modells und mit den Abstraktionsebenen *funktional, logisch* und *konkret* entwickelt. (Kapitel 3.1.1.4) Die Modellstruktur war auf die in PEGASUS betrachtete Kundenfunktion “SAE-Level Level 3 Autobahn-Pilot” hin ausgerichtet. Im Rahmen der Projektarbeit von VVM wurde das 6-Ebenen-Modell auf den VVM Anwendungsfall “urbaner SAE-Level 4 City-Pilot” (siehe Kapitel 3.1.1.3) für eine urbane ODD erweitert. Dies beinhaltet eine modellmäßige Überarbeitung und Erweiterung von Ebenen. Hierzu zählen insbesondere die Ebene 4 und die Ebene 1. Das Konzept des "logischen Szenariomodells" wurde um die Begriffe Szenario "Klasse" und "Instanz" erweitert.

Von einer logischen Szenarioklasse wird gesprochen, wenn die relevanten Parameter zur Beschreibung der Betriebssituationen und -zustände in der ODD (siehe Kapitel 3.1.1.3) in Abhängigkeit von der Kundenfunktion des zu entwickelnden ADS definiert bzw. deklariert sind. Eine Szenarioklasse wird zu einer Szenarioinstanz, wenn für die Parameter der Klasse Wertebereiche definiert oder instanziiert sind. Die Details dieses Verfahrens sind in Abbildung 32 dargestellt.

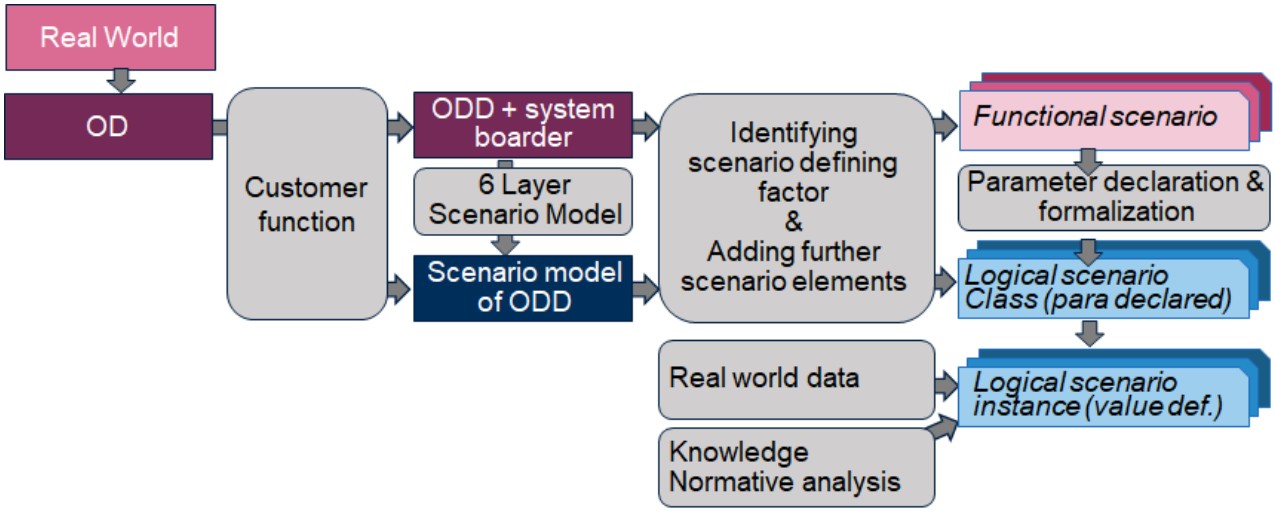


Abbildung 32: Ableitung von Szenarioklassen und Szenarioinstanzen (Realitätsabstraktion)

Das Ergebnis dieses Prozesses ist eine Menge von CORE*-Szenarien (funktional oder logisch in Form von Instanzen). Diese ermöglichen es, die ODD (hier: Verkehrs- und Umgebungs-bedingungen in der Ziel ODD der Kundenfunktion) zu formalisieren bzw. zu modellieren. Die Menge der CORE-Szenarien ist definiert als eine Menge repräsentativer Klassen von funktionalen bzw. logischen Szenarien, die festgelegt sind als:

- die kleinste Menge logischer / funktionaler Szenarien
    - die die bekannten Kategorien von Anwendungsfällen beschreiben, die in der ODD für die Kundenfunktion im Rahmen einer sicheren und konformen Kundenfunktion innerhalb eines sicheren und konformen ODD-Verhaltens auftreten können;
    - deren zugrundeliegende Basisszenarien, die dynamische Basisbewegungs-konstellationen definieren, disjunkt sind;
    - die hinreichend vollständig die ODD repräsentiert;

- für deren Klassen die kleinste Menge von Parametern deklariert wurde, die in jedem Element der Menge der logischen Szenarien die bekannten Kategorien von Parametern repräsentieren, die für die Kundenfunktion in der ODD im Rahmen der logischen Szenarien relevant sind;
- die nach Relevanz/Exposition in der ODD geordnet sind.

Die Core Szenarien bzw. die zugehörigen Klassen und Instanzen können als Ontologie beschrieben werden oder die Basis für die A.U.T.O. Ontologie genutzt werden (siehe Kapitel 3.1.1.4.6). Die A.U.T.O. Ontologie verbindet die dargestellte Szenarienbeschreibungssystematik mit Kritikalitätsphänomenen.

Das ODD-Metamodell umfasst die Menge der funktionalen / logischen CORE Szenarien (Klassen / Instanzen) sowie die Szenariendatenbank.

Das Metamodell für ODD erfüllt die Anforderung zur Dekompositionsfähigkeit der Szenarien:

- das Metamodell ist in CORE-Szenarien zerlegbar,
- jedes CORE-Szenario ist in Beschreibungsebenen zerlegbar,
- jede Beschreibungsebene ist in Kategorien zerlegbar,
- jede Kategorie ist in Parameter zerlegbar.

OD-Domänen-Analyse

Die “Systemanforderungsanalyse" (System Demand Analysis) des V-Modells (Abbildung 33) dient dazu ein detailliertes Verständnis der möglichen Betriebssituationen und Betriebszustände für die zu entwickelnde automatisierte Fahrfunktion (Kundenfunktion) in der geplanten ODD zu entwickeln sowie der dort geltenden gesetzlichen Rahmenbedingungen und vorherrschenden gesellschaftlichen Erwartungen an einen sicheren Betrieb zu bestimmen. Ziel ist ein Verständnis des Raums der Anforderungen.

Im Rahmen der VVM Gesamtmethode wird eine systematische Identifizierung (in VVM als Kritikalitätsanalyse bezeichnet) potenzieller Auslöser für kritische Zustände (in VVM als Kritikalitätsphänomene bezeichnet), in die das zu entwickelnde ADS im Rahmen der möglichen Betriebssituationen und Betriebszustände geraten kann. Ziel ist die Definition der sicherheitsrelevanten Fähigkeiten sowie resultierender Anforderungen an ein sicheres sowie konformes Verhalten des ADS in der gewählten Betriebsumgebung.

Diese Menge der Fähigkeiten und Anforderungen wird im Rahmen des System-Designs immer weiter detailliert und schließlich in technische Komponenten und Architektur eines automatisierten Fahrsystems verfeinert, das so ausgelegt ist, dass es die festgelegten Sicherheits- und Konformitätsanforderungen erfüllt und seine technischen Beschränkungen erkennt.

Diese Menge der Fähigkeiten und Anforderungen wird im Rahmen der Validierung und Verifikation zum Nachweis des sicheren und konformen Verhaltens des Systems mit einem akzeptablen Restrisiko verwendet.

Das ODD-Metamodell ermöglicht es, dies durchgängig szenarienbasiert zu tun.

Das detaillierte "Problemraumverständnis" wird verwendet, um methodisch das Auftreten von gefährlichen und auslösenden Ereignissen in der Menge der CORE-Szenarien aus dem ODD-Metamodell zu identifizieren. Dabei werden nicht nur der Ausfall oder nicht beabsichtigte Funktionalitäten der automatisierten Fahrfunktion, sondern auch inhärente Gefährdungen (Hazards) bzw. ihre auslösende Ereignisse (hazardous events) in der System-Fahrzeug-Umwelt-Interaktion (szenariobasiert beschrieben durch das ODD-Metamodell) systematisch betrachtet und zu vermeidende Ereignisse ermittelt.
Methoden, um den Problemraum zu analysieren und relevante Phänomene zu identifizieren, sind z.B. Robustheitsanalysen in der Simulation, die Auswertung von vorhandenem Wissen und Expertenwissen, einschließlich der Analyse von Unfalldatenbanken und Felddaten. Ein weiteres Beispiel ist die Expertenanalyse. Das zugrundeliegende methodische Vorgehen wird in VVM als "Kritikalitätsanalyse" bezeichnet. (siehe Kapitel 3.1.1.6 Kritikalitätsanalyse) Im Rahmen der Analyse der ODD werden in den Parameterräumen der CORE Szenarien Bereiche für nominales, risiko-, gefahren und fehlerbehaftetes Verhalten identifiziert.

Im Rahmen der ODD/Domänen Analyse werden die notwendigen Systemfähigkeiten des ADS definiert, die ODD spezifisch unter Berücksichtigung der in der ODD geltenden gesetzlichen sowie ethischen / gesellschaftlichen Rahmenbedingungen erfüllt sein müssen, damit vom/für ADS kein unangemessenes Risiko in seiner Operational Design Domain (ODD) ausgeht. Zunächst werden systemunabhängige Top Goals erarbeitet. Dazu zählen Leitlinien sowie entwicklungsrelevante Anforderungen. Die Leitlinien für die ADS-Entwicklung und Absicherung werden im Kontext von VVM beispielsweise aus den Sub-Goals 1 bis 4 (siehe Abbildung 28) abgeleitet. Sie definieren einen generellen Rahmen etwa für das Verhalten und Fähigkeiten mit Orientierungsmaßstäben, wie der Ableitung des Niveaus eines akzeptablen Risikos, Risikomodellen, Evaluationsmaße und ein Konzept für die Erzeugung von Evidenzen im Rahmen der Validierung und Verifikation, sodass argumentiert werden kann, dass das Niveau des Restrisikos den gesellschaftlichen und rechtlichen Erwartungen entspricht.

Diese entwicklungsrelevante Richtlinie wird szenarienbasiert zu Anforderungen für die Auslegung des sicheren und konformen Systemverhaltens sowie der notwendigen Performance heruntergebrochen. Dieser konsistente Anforderungsrahmen für die Systemauslegung integriert die Aspekte, die sich aus den Sichtweisen des Herstellers, des Rechtsrahmens, der Gesellschaft unter Bezugnahme der Zertifizierungsregularien und anderen Stakeholderperspektiven ergeben. Die Sicherheitsmaßnahmen, die notwendig sind um dies zu untermauern, werden im Prozessschritt Leistungs- & Verhaltensspezifikation (Abbildung 31, siehe auch Kapitel 3.1.1.7 Fähigkeitsanalys & Verhaltensspezifikation) für das ADS definiert und in Folgeschritten implementiert, verifiziert und validiert, um ein unzumutbares Risiko zu verhindern.
Dabei werden Klassen von Szenarien definiert und analysiert, in denen das System arbeiten soll, um die dominierenden Merkmale in dem Szenario zu identifizieren, die einen relevanten Einfluss auf ein sicheres Verhalten des Gesamtsystems haben. Eine zentrale Herausforderung bei der Gewährleistung der Sicherheit des hochautomatisierten Fahrens ist die Sicherstellung eines ausreichenden Maßes an Zuverlässigkeit, dass alle möglichen systematischen Auslöser und gefährlichen Ereignisse zum Zeitpunkt der Freigabe des Systems in seinem ODD bekannt sind und beherrscht werden.

Die VVM-Gesamtmethode integriert daher die Teilaufgaben Risikoanalyse, Risikobewertung und Risikobehandlung zur Sicherstellung der Systemleistung innerhalb der Risikoakzeptanz. Ergänzt werden diese Themen durch das prozessbezogene Management des "Restrisikos", das unter einem akzeptablen Niveau gehalten werden muss, damit das ADS als sicher gilt. Die

prozessbedingt erforderliche Risikominderung bestimmt den Umfang der Sicherheitsmaßnahmen, die ergriffen werden, um die Schwere oder Wahrscheinlichkeit eines Schadens auf das definierte akzeptable Restrisiko zu reduzieren. Der Szenarienkatalog, für den das tatsächliche Risiko des Systems gemanagt werden muss, ist das ODD-Metamodell (CORE-Szenarien).

Das funktionale Systemverhalten der automatisierten Fahrfunktionen und der dafür notwendigen Systemfähigkeiten werden typischerweise durch die Spezifikation ihres Verhaltens in Use- und Non-Use-Cases beschrieben. Hierzu wird die Kundenfunktion rekursiv in (detaillierte funktionale) Wirkketten heruntergebrochen. Basierend auf den CORE-Szenarien des ODD-Metamodells kann die funktionale Beschreibung des Systems daher in Form einer Reihe von funktionalen Anwendungsfällen definiert werden, die das beabsichtigte funktionale Verhalten, eine funktionale Domäne und die Definition von Grenzen definieren. Szenarien eignen sich gut für die Beschreibung von Testfällen, indem die Szenariobeschreibungen um Pass/Fail-Kriterien erweitert werden.

Eine erste Erweiterung der durch Use Cases definierten Kundenfunktion und ihrer Wirkketten ist die Integration einer Reihe von Anforderungen, die die Bedürfnisse der Stakeholder, wie z.B. rechtliche, soziale und ethische Anforderungen, aber auch Erwartungen des Fahrers an das beabsichtigte Verhalten des Systems in den CORE-Szenarien repräsentieren. Diese Anforderungen müssen nachvollziehbar definiert sein und eine klare Definition der Grenzen des Systemverhaltens in Bezug auf diese Randbedingungen enthalten.

In diesem Zusammenhang ist es notwendig, einen nachvollziehbaren Prozess innerhalb der Gestaltung eines ADS zu etablieren, der die teilweise situativ widersprüchlichen Anforderungen, die sich u.a. aus fahrerischen, rechtlichen, sozialen, ethischen und haftungsrechtlichen Anforderungen ergeben, abwägt. Dieser Prozess muss die daraus resultierenden Risiken ermitteln und im Falle von Abweichungen aufgrund einzelner notwendiger Verhaltensentscheidungen das daraus resultierende zusätzliche Risiko für den Hersteller transparent machen.

Die Rückverfolgbarkeit von entwicklungsrelevanten Anforderungen insbesondere von sicherheitsrelevanten, verhaltensrechtlichen sowie zertifizierungsrelevanten System- und Prozessanforderungen ist notwendig. Sie werden beispielsweise bei der Spezifikation des Soll-Verhaltens durch die Semantische-Norm-Verhaltensanalyse und das Phänomen-Signal-Modell prozessual unterstützt. Die Rückverfolgbarkeit von der Verhaltensspezifikation zum Systementwurf werden durch eine strukturierte, dekomponierte Spezifikation der Anforderungen an Systemfähigkeiten gewährleistet.

Integration *Risikomanagementkern* (Risk Management Core; RMC)
Im Rahmen des System-Designs (Abbildung 33) wird ein iterativer Ansatz zur Verfeinerung der Sicherheitsziele in Abstimmung mit den Entscheidungen zur Ableitung von Systemfähigkeiten sowie der funktionalen und verhaltensbasierten Sicherheitsanforderungen (safety behavior requirements, siehe Kapitel 3.1.1.7 Fähigkeitsanalyse und Verhaltensspezifikation) angewendet. Um auch hier eine geeignete Evidenz zur Argumentation nutzen zu können, wird der Risk Management Core als Werkzeug bei der Systementwicklung integriert. In jeder Verfeinerungsstufe werden die Annahmen des Entwurfs explizit dargestellt und analysiert, sodass sie später auch validiert werden können. Insgesamt wird ein funktionaler und technischer Systementwurf abgeleitet, der in der Lage ist, die Sicherheitsziele auch bei unvermeidbaren Unzulänglichkeiten und Fehlern in einzelnen Komponenten zu erreichen. Dies ermöglicht zudem die durchgängige

Verwendung von gleichen Risikomodellen, Evaluierungsfunktionen und Risikoakzeptanzlevel im gesamten Entwicklungsprozess (V-Modell).

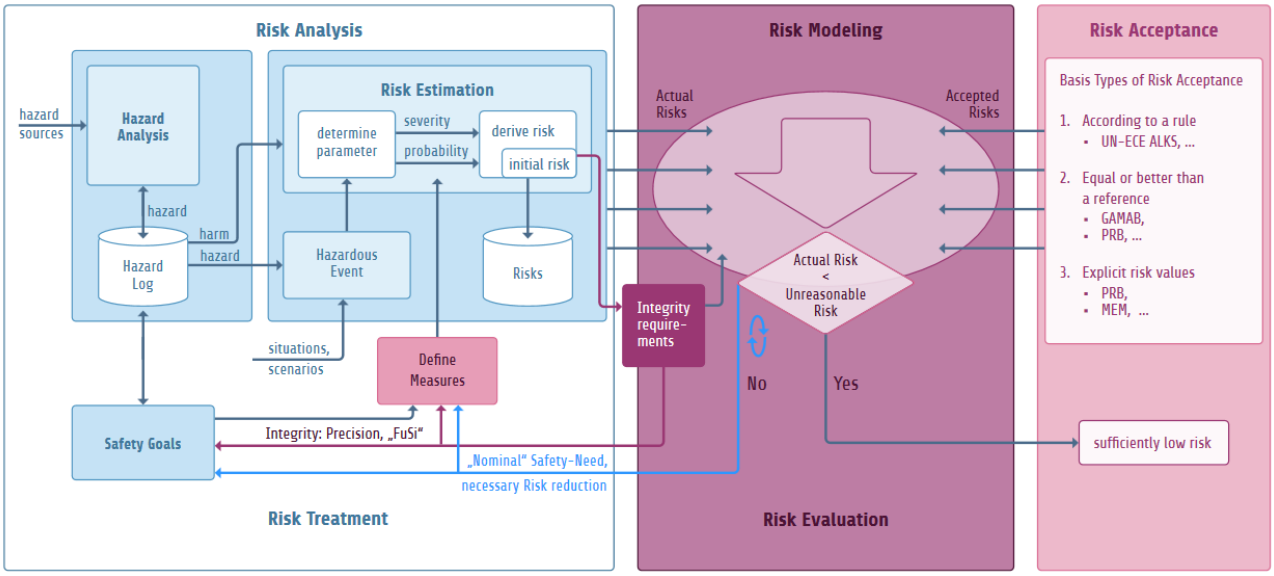


Abbildung 33: Der Risk Management Core

VVM integriert die Idee der konsequenten Anwendung von kontrolliertem und gemanagtem Risiko während des gesamten Design- und Absicherungsprozesses. Der *Risikomanagementkern* (RMC) ist ein iterativer Prozess. Er dient dazu, das tatsächliche Risiko einer Sicherheitsmaßnahme zu bewerten und mit dem akzeptierten Risiko abzugleichen. Der RMC unterstützt die explizite Darstellung und Behandlung von Risiken in gefährlichen oder auslösenden Ereignissen, die in Szenarien enthalten sind, die zu gefährlichem Verhalten führen.

Bewertung des Risikos im Rahmen RMC

Um das tatsächliche Risiko und das akzeptierte Risiko für das System in Einklang zu bringen, ist es notwendig, Kriterien für eine Risikoakzeptanz von ODD zu definieren.

Zu den ethischen Aspekten des automatisierten Fahrens hat in Deutschland das Bundesministerium für Verkehr und digitale Infrastruktur 2017 ein Gutachten in Auftrag gegeben. Eine der Empfehlungen der Ethik-Kommission “Automatisiertes und vernetztes Fahren” war, dass der Nachweis erbracht werden müsse, dass automatisierte Fahrsysteme in Bezug auf die Vermeidung oder Verringerung von Schäden in Gefahrensituationen „… im Vergleich zu menschlichen Fahrleistungen zumindest eine Verminderung von Schäden im Sinne einer positiven Risikobilanz entspricht ... wobei der Schutz von Menschen Vorrang vor allen anderen Nützlichkeitserwägungen hat… und die Vermeidung von Unfällen Leitbild ist, wobei technisch unvermeidbare Restrisiken einer Einführung des automatisierten Fahrens bei Vorliegen einer grundsätzlich positiven Risikobilanz nicht entgegenstehen“ [49].

Ein ähnlicher Ansatz, der auf der französischen Definition „globalement au moins aussi bon“ basiert, verweist auf das Prinzip, dass jedes neue System mindestens so gut sein muss wie das vorherige, das es ablöst.

In der PEGASUS Methodik wurde als Risikoakzeptanzkriterium die positive Risikobilanz in Kombination mit dem zusätzlichen Kriterium verwendet, dass im Fall eines Unfalls eines

Fahrzeugs, das mit einem ADS ausgestattet ist, dies nur dann akzeptabel ist, wenn die Systemleistung mindestens der des Medians der menschlichen Leistung entspricht. Die VVM-Methode übernimmt dies. Sie verwendet die gleiche Risikobewertung im RMC sowie in der Validierung und Verifikation.

Spezifikation des Sollverhaltens auf der Grundlage eines akzeptablen Risikos.

Im Rahmen der Spezifikation des Sollverhaltens des ADS ist der RMC ein Kernelement um argumentieren zu können, dass der Prozess der Spezifikation des Sollverhaltens des ADS eine risikobasierte (Soll-) Verhaltensspezifikation liefert, die die Anforderungen an ein sicheres Verhalten einschließlich der erforderlichen Integrität enthält.

Im Rahmen der Argumentation des ADS-Safety Cases ist es notwendig, schlüssig belegen zu können, dass der Prozess der Spezifikation des Sollverhaltens eine risikobasierte Verhaltensspezifikation liefert, die die Anforderungen an die Verhaltenssicherheit einschließlich der erforderlichen Integrität enthält. Die ISO 21448 verlangt eine solche Argumentation für das Nichtvorhandensein eines unangemessenen Risikos aufgrund von Unzulänglichkeiten. Unzulänglichkeiten können aus mangelhaft spezifizierten Anforderungen an Verhalten oder Performanz resultieren. Der in die VVM-Gesamtmethode integrierte Ansatz zur risikobasierten Verfeinerung der funktionalen Spezifikation (siehe Abbildung 34) setzt auf die Ergebnisse des vorherigen Schrittes System Demand Analysis gemäß V-Modell (siehe Abbildung 27) auf. Die folgende Darstellung lehnt sich eng an [50] an. Details finden sich in Kapitel 3.1.1.7 Fähigkeitenanalyse und Verhaltensspezifikation.

Die Verhaltensspezifikation ist Teil der funktionalen Spezifikation des ADS. Der auf der Integration des RMC basierende Ansatz zur risikobasierten Verfeinerung der funktionalen Spezifikation (Abbildung 34) erfordert eine Methode zur Ableitung einer formalen Spezifikation des Zielverhaltens.

In VVM wurden exemplarisch zwei Ansätze entwickelt, die es ermöglichen, getroffene Annahmen und daraus resultierende Entscheidungen in einer Verhaltensspezifikation zu formulieren. Dies sind das „Phänomen-Signal-Modell“ (PSM) und die „Semantische Norm Verhaltensanalyse“ (siehe Kapitel 3.1.1.7 Fähigkeitsanalyse und Verhaltensspezifikation). Beide formalen Ansätze aber auch eine interdisziplinäre Expertengruppe, die nach einem festen Regelwerk arbeitet, ermöglichen die nachvollziehbare (szenariobasierte) Ableitung von formalen Anforderungen an das Systemverhalten (in den Betriebsszenarien und Zuständen der ODD) aus Verkehrsgesetzen sowie die Integration von Annahmen/Fakten (z.B. über das Verhalten von anderen Verkehrsteilnehmern in den Szenarien) sowie Regeln, die sich aus weiteren Stakeholderbedürfnissen (z.B. ethische Anforderungen an das Systemverhalten, Zulassungsrecht, Stand der Technik) ergeben. Die Kombination von Fakten und Regeln ergibt eine formale Spezifikation des ADS-Sollverhaltens in Form von Anforderungen, die als Input in den RMC verwendet wird.

Die Identifikation von gefährlichem Sollverhalten erfolgt durch eine risikobasierte Verfeinerung der funktionalen Spezifikation sowie durch den Abgleich mit zuvor identifizierten Gefährdungen (Hazards) oder auslösendem Bedingungen von gefährlichem Verhalten (siehe Abbildung 34). Funktionale Mängel werden aufgezeigt und explizit mit risikomindernden Maßnahmen (qualitativ und quantitativ) versehen. Wenn das Risikoniveau des identifizierten Sollverhaltens nicht akzeptabel ist, werden Zielvorgaben für ein sicheres Verhalten (Sicherheitsziele) definiert. Die abgeleiteten Sicherheitsziele umfassen die erforderliche qualitative und quantitative Risikominderung, woraus dann Sicherheitsmaßnahmen abgeleitet werden. Wenn die Maßnahmen

für das Sollverhalten akzeptabel und durchführbar sind, wird in einer ersten Iterationsschleife mit dem RMC das funktionale Sollverhalten risikobasiert festgelegt (Abbildung 34 Schritt 4). In der ersten Iterationsschleife werden die spezifizierten Risikominderungsmaßnahmen in die Verhaltensspezifikation integriert, gefolgt von einer weiteren Risikoanalyse des Sollverhaltens (Abbildung 34 Iteration 1). Wenn dieser erste Iterationsschritt Maßnahmen ergibt oder erfordert, die im Rahmen der Verhaltensanpassung nicht umsetzbar sind, werden alternative Maßnahmen definiert, die geeignet sind, das angestrebte Sicherheitsziel zu erreichen (z.B. Anpassung der ODD durch Definition angepasster Systemgrenzen).

Nachdem in der ersten Iterationsschleife das Sollverhalten und alle abgeleiteten Sicherheitsziele sowie Maßnahmen (die Formulierung geeigneter Requirements) in der Verhaltensspezifikation so angepasst wurden, dass das Restrisiko des Sollverhaltens des betrachteten ADS akzeptabel ist, beginnt eine zweite Iterationsschleife (Abbildung 34 Iteration 2). Nun werden in gleicher Weise diejenigen Auslösebedingungen analysiert, die zu ungewünschten Abweichungen vom Sollverhalten führen können. Wenn sich die Abweichungen als gefährlich erweisen, muss das Risiko, das sich aus einem solchen Verhalten ergibt, in Form von Eintrittswahrscheinlichkeit und Schweregrad quantifiziert werden. Für das Bestehen der Iteration 2 (Abbildung 34) muss das Risiko aus dem Sollverhalten kleiner als das akzeptable Risikoniveau sein.

Eine weitere Verringerung des Risikos durch risikobasierte Anpassungen des Sollverhaltens ist erforderlich, wenn die Risikobewertung eine Verletzung des Kriteriums der Risikoakzeptanz ergeben hat. Risiken, die sich aus den spezifizierten Sicherheitsmechanismen ergeben, werden notwendigerweise in Iteration 1 (Abbildung 34) berücksichtigt. Eine verfeinerte Verhaltensspezifikation kann erstellt werden, wenn alle Risikoakzeptanzkriterien durch die Verhaltensspezifikation erfüllt werden, einschließlich Risikominderung und Sicherheitsintegrität.

Am Ende muss sichergestellt werden, dass das spezifizierte (Sicherheits-) Verhalten, mit dem sich aus der Problemraumanalyse ergebenden notwendigen Anforderungen deckt und widerspruchsfrei ist (Spezifikationslücke). Die szenarienbasierte Vorgehensweise ermöglicht die explizite Einbeziehung von Experten in den iterativen Entwicklungs- bzw. Reviewprozess.

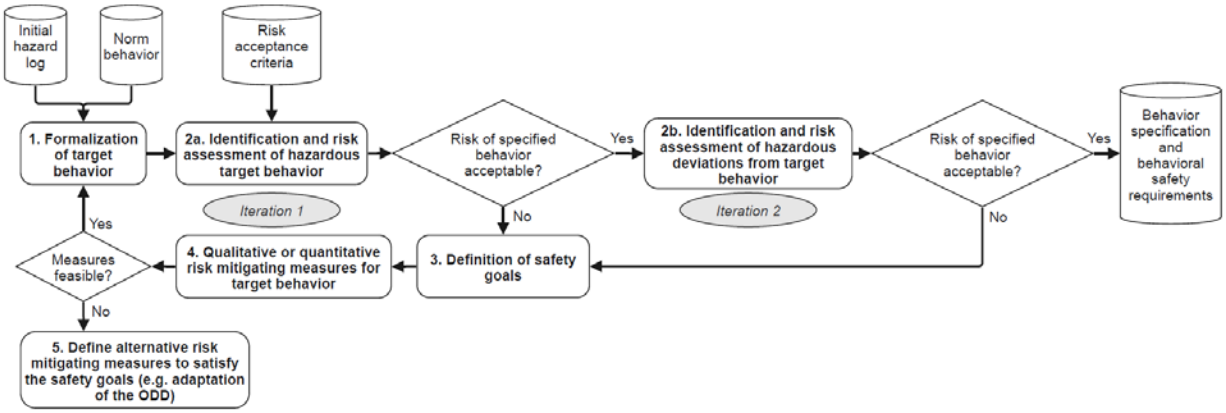


Abbildung 34: Prozess zur Ableitung einer risikobasierten Verfeinerung funktionaler Spezifikationen , der als Evidenz für die Argumentation ein sicheres integres Sollverhalten liefert [49].

Der Fluss von Anforderungen und Sollverhalten zur Architektur

Das Sollverhalten des ADS wird durch Systemanforderungen spezifiziert. Diese setzen sich aus funktionalen (Sicherheits-) Anforderungen und Verhaltensanforderungen (an ein sicheres Verhalten) zusammen, wobei Verhaltensanforderungen ebenfalls Sicherheitsanforderungen darstellen können.

Die verhaltensbezogenen Sicherheitsanforderungen spezifizieren das lösungsunabhängige sicherheitsrelevante Verhalten oder die lösungsunabhängigen Sicherheitsmaßnahmen, einschließlich der sicherheitsbezogenen Attribute, die den Grad der erforderlichen Risikominderung und Integrität angeben. Beim funktionalen Entwurf werden die verhaltensbezogenen Sicherheitsanforderungen in einen eindeutigen Satz funktionaler Sicherheitsanforderungen übersetzt. Diese können aus Performanzanforderungen bestehen, die technische Werte zur Definition der Systemleistung enthalten. Durch die Bewertung der Systemleistung mit Hilfe eines szenariobasierten Ansatzes wird ein Abgleich zwischen den Qualitätsmaßstäben der verhaltensbezogenen Sicherheitsanforderungen und den Leistungsanforderungen erreicht. Eine solche Bewertung stellt - zurück auf der Ebene des Verhaltens - die Grundlage für die Abschätzung der Restrisiken dar. Die (System-) Performance-Anforderungen werden bei der Verifikation zu Testkriterien in Testfällen, hierzu werden Pass/Fail-Kriterien spezifiziert und hinzugefügt. Die Nachvollziehbarkeit wird durch ein Anforderungsmanagementsystem sichergestellt.

Die Systemanforderungen werden verwendet, um eine funktionale Architektur zu definieren. Ziel ist es, die Funktionalitäten so zu gruppieren, dass die Architektur, d.h. das hierarchische Konstrukt der Funktionalitäten, in seine Bestandteile zerlegt werden kann. Während der Spezifikation der funktionalen Architektur werden auch die Systemanforderungen verfeinert.

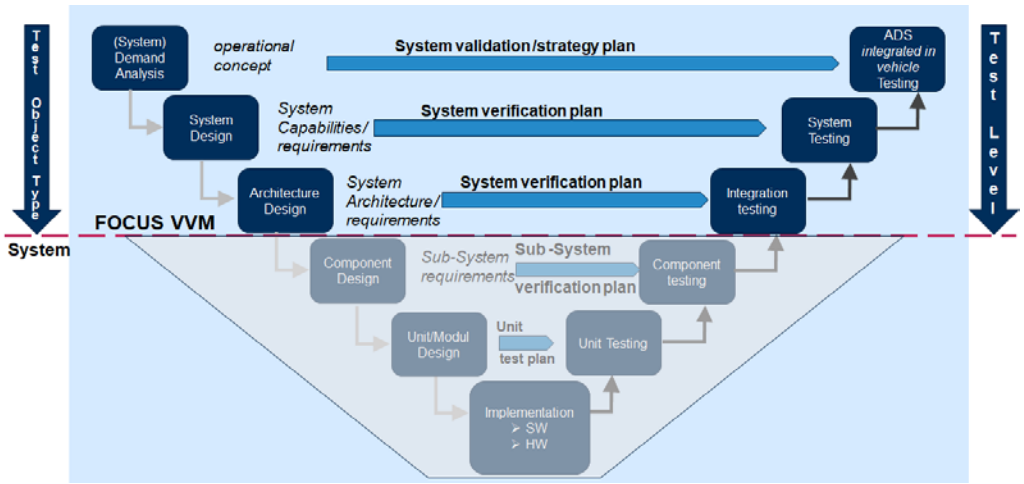


Abbildung 35: Beispielhaft gewählte Tiefe der Beschreibung der Inhalte der VVM-Methode (Entwicklung & Test)

Am Ende muss verifiziert werden, dass spezifiziertes Verhalten und Architektur eine exakte Darstellung des beabsichtigten und in der SW/EE und HW implementierten Requirements sind. Szenarien, die auf dem ODD-Metamodell basieren, ermöglichen die explizite Einbeziehung von Experten in den iterativen Entwicklungsprozess, um vor dem Testen die Implementierungslücke zu bewerten. Im Rahmen der Argumentation des ADS-Safety Cases, ist dies auch mit Evidenzen im Test- und Absicherungskonzept im Rahmen der Verifizierung und Validierung der “Operational Safety & Conformity” des ADS-Releases zu gewährleisten. Dass dies ein mehrstufiger Prozess ist,

zeigt beispielhaft die Abbildung 36. Sie zeigt die formale Verifikation des implementierten Verhaltens gegenüber dem Spezifizierten, wie es beispielweise in Audits vor dem Überprüfen durch Tests stattfindet.

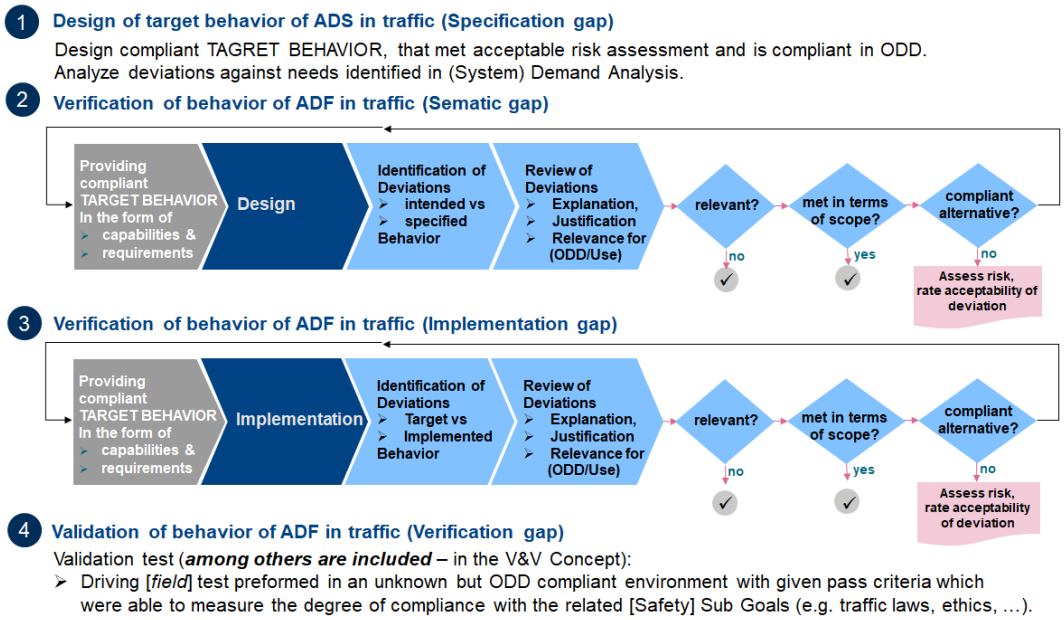


Abbildung 36: Beispielhafte Vorgehensweise zur Vermeidung von Transfer-Lücken und Divergenzen im Entwicklungsprozess

In jedem Entwicklungsschritt des V-Modells werden Entscheidungen getroffen, um Anforderungen zu definieren und sie in dem nächsten Schritt auszudetaillieren. Im Rahmen der Implementierung werden sie in Hardware oder Software umgesetzt. Auch in diesem Prozessschritt werden Entscheidungen getroffen. Die getroffenen Entscheidungen sind nachvollziehbar zu dokumentieren. Neben ihrem Risikobeitrag sind sie auch in Bezug auf gesellschaftliche, ethische und technische Compliance sowie Umsetzungslücken (Implementierungslücke) zu überprüfen.

Adventive Elemente für die Phase der Validierung und Verifizierung

Das **ODD-Metamodell** wird ergänzt, um das V-Modells durchgängig szenariobasiert gestalten zu können. Damit ist es möglich, die Absicherung des ADS mit denselben, die ODD valide repräsentierenden Szenarienklassen, durchzuführen wie die Entwicklungsphase und das Datamining auf Messdaten.

> Dadurch ist eine neue Aufgabe der V&V entstanden. Es ist die ausreichende Validität der Menge der CORE-Szenarien zu überprüfen, d.h. der Nachweis, dass die CORE-Szenarien und die zugehörigen Klassen eine adäquate Abdeckung der tatsächlichen Szenarien, die in der Zieldomäne vorkommen, darstellen.

Die **Evaluierung des verbleibenden Risikos** wird hinzugefügt, weil es ist wichtig ist das Niveau des von einem mit ADS ausgestatteten Fahrzeugs in seiner Zielbetriebsdomäne ausgehenden Risikos sicherzustellen.

Das **V&V-Konzept** wird durch Evidenzen ergänzt, die belegen dass der Betrieb eines mit ADS ausgerüsteten Fahrzeugs in seinem bestimmungsgemäßen Betriebsbereich mit vertretbaren Risiken für Fahrer, Beifahrer und andere Verkehrsteilnehmer verbunden ist.

Abbildung 37 zeigt eine modifizierte Darstellung des V-Modells aus Abbildung 27. Es wurden die zuvor definierten (Kern-) Elemente für die Entwicklungsphase eines ADS integriert.

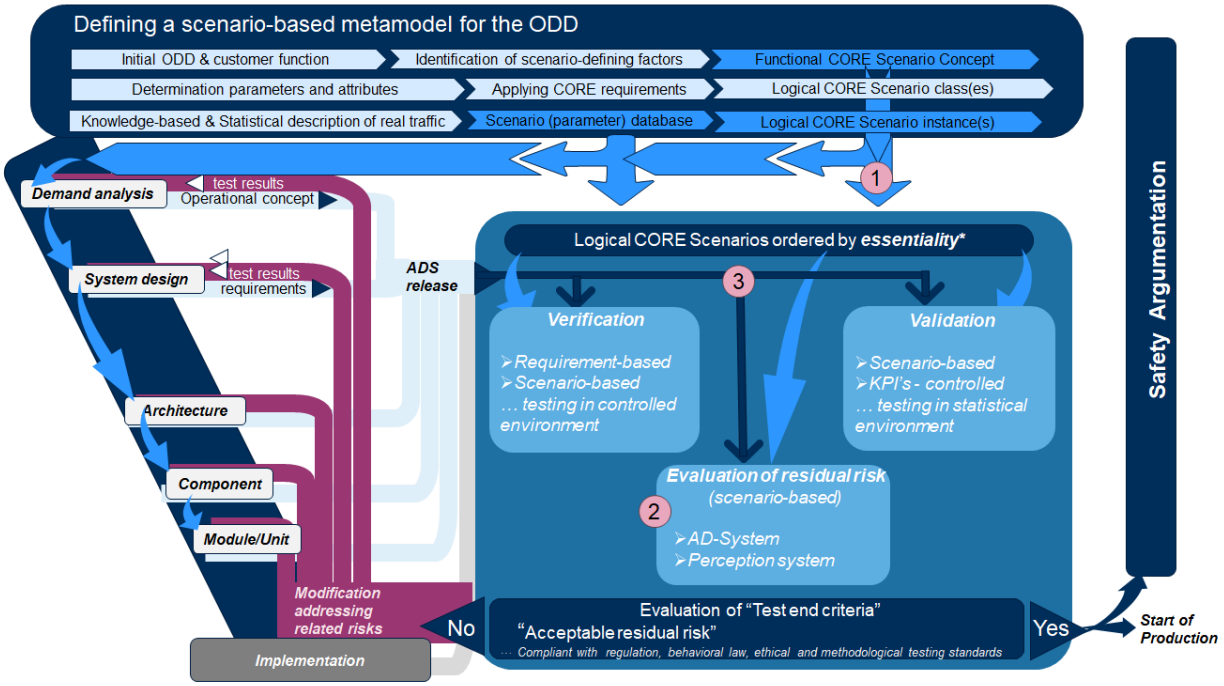


Abbildung 37: V-Modell (modifizierte Darstellung) mit den adventiven (Kern-) Elementen der VVM-Gesamtmethode in der Phase der Validierung und Verifikation (rechte Seite V-Modell)

V&V Konzept

Das V&V-Konzept definiert eine Verifizierungs- und Validierungsstrategie, die das Risiko potenziell gefährlicher Auslöseereignisse für eine unbeabsichtigte Auslösung des ADS bewertet. Dabei werden die Risiken bewertet in Bezug auf

- die Fähigkeit der Sensoren und Sensordatenverarbeitungsalgorithmen die Umgebung zu modellieren,
- die Fähigkeit der Entscheidungsalgorithmen mit bekannten und unbekannten Situationen umzugehen und angemessene Entscheidungen zu treffen und
- im Bezug auf die Fähigkeit der Mensch-Maschine-Schnittstelle vorhersehbaren Missbrauch zu verhindern.

Das Verifikationskonzept und das Validierungskonzept definieren die Testkonzepte für das ADS. Das V&V-Konzept verbindet dabei die Testobjekte, Testziele, Teststufen, Testplattformen und Teststrategien. Die Validierungsziele liefern den Nachweis, dass das Risiko für Fahrer, Insassen und andere Verkehrsteilnehmer während des Betriebs im definierten ADS akzeptabel ist und mit hinreichender Zuverlässigkeit erfüllt wird. Die Verifikationsergebnisse bestätigen, dass die Validierungsziele für bekannte Gefahrenszenarien erreicht werden und dass das Restrisiko aus bekannten Gefahrenszenarien nicht unangemessen ist.

Der erste wichtige Schritt im Rahmen des V&V besteht darin, zu überprüfen ob alle Anforderungen, die aus "Safety by Design" abgeleitet wurden, erfüllt sind. Dieser Schritt stellt

sicher, dass bekannte Szenarien abgedeckt sind und dass sich das System in ihnen wie erwartet verhält.

Die Verifikation konzentriert sich somit auf überprüfbare Anforderungen und kann dabei auf etablierte "Safety by Design"-Prozesse für Fahrwerks- und Assistenzsysteme zurückgreifen, die bereits seit Jahrzehnten in der Entwicklung vom Serienfahrzeugen integriert sind. Bei der Verifikation werden die aus dem Designprozess erzeugten Anforderungen an Gesamt-und Subsysteme anhand genereller Testziele und Teststrategien geprüft.

Die Validierung zielt darauf ab, die statistischen Argumente für die Bestätigung der Sicherheit in bekannten und unbekannten Szenarien mit ausreichendem Vertrauen aufzubauen. Dies ist der zweite Schritt des V&V-Prozesses. Bei der Validierung wird das zu prüfende System in Szenarien oder Situationen getestet, denen das System nach seiner Freigabe im täglichen Straßenverkehr wahrscheinlich begegnen wird.

Das Konzept des Restrisikos ist seit langem akzeptiert (siehe die Einführung von Airbags, Notbremssystemen oder neuen Medikamenten). Der dritte Schritt, die Evaluierung des Restrisikos, überprüft das Risikolevel des ADS-Release und vergleicht es mit dem Akzeptanzlevel. Das Risikolevel des ADS-Release wird über statistische Verfahren ermittelt. Die Grundlage der statistische Verfahren werden im Validierungsprozess gesetzt.

Szenariobasierte Verifikation

Bei der Verifikation wird durch objektive Nachweise (d.h. Prüfung und Bewertung) nachgewiesen, dass die in der Phase der Entwicklung spezifizierten Anforderungen an das ADS durch Umsetzung in der Phase der Implementierung erfüllt werden. Dies entspricht zum einen der Überprüfung der sachgerechten Implementierung und zum anderen auch der Überprüfung der Implementierungs-lücken. Im Idealfall ist das ADS bzw. die Integration des ADS in ein Fahrzeug spezifizierungs-konform. Die szenariobasierte Verifikation ermöglicht dabei eine gesamtsystemische Prüfung in welcher die Summe einzelner Spezifikationen über einen zeitlich- und räumlich ausgedehnten Prüfraum (das Szenario) in ihrem Zusammenwirken betrachtet wird. Dadurch können u.a. die obengenannten Spezifizierungslücken identifiziert werden. Außerdem wird der Nachweis erbracht, dass das Gesamtsystem / die Komponenten (die Testobjekte) keine unerwünschten Funktionalitäten oder Betriebseigenschaften enthalten, die ein generelles Sicherheitsziel verletzen könnten.

Die Verifikation der Funktionalität und Integration stellt sicher, dass alle sicherheitsrelevanten Funktionen und Sicherheitsmechanismen in den bekannten Szenarien-Instanzen (beschrieben durch das ODD-Metamodell) frei von unakzeptablen Risiken sind. Die Systemverifikation konzentriert sich auf die Beurteilung des (robusten) Verhaltens (z.B. Funktionalität, Performance, Reaktion auf Systemgrenzen, Interaktion an Schnittstellen, …) des ADS in Bezug auf bekannte auslösende Ereignisse. Es wird bewertet, ob das Restrisiko für gefährliche Ereignisse aufgrund bekannter Unzulänglichkeiten ausreichend gering ist.

Die Spezifikation der Anforderungen an das System erfolgte im Rahmen der VVM-Gesamtmethodik durchgängig szenariobasiert unter Nutzung des ODD-Metalmodells. (siehe auch Kapitel 3.1.1.5 Szenarienabstraktion - Szenariobasiertes Testen und Kapitel 3.1.1.8 Requirement breakdown) Im Zuge der Verifikation innerhalb der VVM-Gesamtmethodik wird dieser Ansatz konsequent zur szenariobasierten Verifikation weiterentwickelt. Die szenariobasierte Verifikation im Rahmen der VVM-Methodik erfolgt dabei durch anforderungsbasierte Verifikation des

implementierten Verhaltens / Systems gegen die Requirements der ADS-Spezifikation im Szenarien- und Parameterraum der CORE-Szenarioinstanzen und mit der Nutzung der Szenario-(Parameter) Datenbank. Es legt die Grundlage für den Sicherheitsnachweis für die Domäne "Operational Safety & Conformity". (siehe auch Kapitel 3.1.1.5 Realitätsabstraktion - Szenariobasiertes Testen)

Verifikationskonzept

Das Verifikationskonzept definiert die Vorgehensweise zur Verifikation des Systembetriebs und zum Nachweis der korrekten Umsetzung aller Anforderungen und Spezifikationen.
Es definiert, was getestet wird (Testobjekt), für welche Zwecke der Test die Erfüllung nachweisen soll (Testziele), auf welchen Ebenen die verschiedenen Systemelemente getestet werden (Teststufen). Es enthält allgemeine Teststrategien für "anforderungsbasiertes" Testen, die verwendeten Testumgebungen (Testplattformen) und eine Testmatrix mit einer detaillierten Zuordnung der durchgeführten Tests zu den Systemanforderungen.

Generelle Testziele beschreiben Prüfgebiete unabhängig von einer konkreten Prüfebene und gelten für alle Prüfobjekte sowie für alle Prüfobjekttypen. Die generellen Testziele definieren Kriterien, anhand derer überprüft wird ob das Produkt und die Testobjekte korrekt, vollständig und konsistent gemäß der Spezifikation sind und ob sie den Sicherheitsanforderungen nach ISO 26262 und ISO 21448 entsprechen.

Die Teststrategie folgt dem Ansatz des anforderungsbasierten Testens und hat das Ziel, die korrekte Umsetzung dieser Anforderungen nachzuweisen. Bei der Ableitung von Testspezifikationen und Testfällen auf Basis der Anforderungen stellt sich die Frage, ob der spezifizierte Test einen signifikanten Beitrag zur Verifikation leisten kann, d.h. ob die „richtigen“ Tests spezifiziert werden (Qualität des Tests).

Eine Orientierung für die Korrektheit des Testfalls geben die Testziele. Testziele beschreiben, welche (Qualitäts-)Eigenschaften in einem Testobjekt überhaupt nachgewiesen werden sollen. So können z.B. verschiedene Qualitätsmerkmale und -kriterien erst dann geprüft werden, wenn das Testobjekt einen bestimmten Reifegrad erreicht hat. Ein intensiver Funktionstest für ein A-Muster macht keinen Sinn, wenn die zu testende Funktion nur rudimentär implementiert ist. Andererseits muss die Teststrategie sicherstellen, dass die notwendige Überprüfung eines Qualitätsmerkmals nicht unterbleibt, d.h. dass alle Testziele abgedeckt werden. Die Testziele definieren Verifikationskriterien, anhand derer überprüft wird, ob das Produkt und die Testobjekte korrekt, vollständig und konsistent mit ihrer Spezifikation sind und ob sie die Sicherheitsanforderungen nach ISO 26262 erfüllen. Außerdem muss der Nachweis erbracht werden, dass die Testobjekte keine unerwünschten Funktionalitäten oder Betriebseigenschaften enthalten, die ein generelles Sicherheitsziel verletzen könnten.

Generelle Testziele sind insbesondere

- Nachweis der korrekten Funktionalität
- Nachweis der korrekten Funktion der Sicherheitsmechanismen sowie der Mechanismen zur Fehlererkennung und Fehlerbehandlung
- Nachweis der System - Effizienz / Leistungsfähigkeit
- Nachweis der korrekten Funktionalität der “Safety of the Intended Functionality”

- Nachweis der Gebrauchstauglichkeit.

Die Verifikation wird schrittweise von den kleinsten Einheiten bis auf die Ebene des in ein Fahrzeug integrierten ADS statt. Es wechseln sich Komponenten- und Integrationstest ab. Die Struktur findet sich in Abbildung 35.

Das Verifikationskonzept stellt die Konformität zu den Normen und Standards insbesondere mit den Normen ISO 26262 [8][] und ISO 21448 [48] sicher. Testen ist die systematische, abdeckungsorientierte, strukturierte und methodische Durchführung von Tests, die durch Testfallspezifikationen definiert sind.

Konkretisierung der Verifikation

Das System und seine Komponenten (Sensoren, Algorithmen und Aktoren) werden verifiziert, um nachzuweisen, dass sie sich innerhalb der spezifizierten ODD, insbesondere in bekannten/unsicheren Parameterteilräumen von Szenarien, erwartungsgemäß bzw. spezifikationskonform verhalten.
Weiterhin muss nachgewiesen werden, dass das ADS und seine Komponenten keine unerwünschten Funktionalitäten oder Betriebsmerkmale aufweisen und keine generellen Sicherheitsziele verletzen.
Im Zusammenhang mit der Verifikation der Funktionalität des ADS können durch szenariobasiertes Testen unter Verwendung des Metamodells für das ADS die etablierten Testziele wie die korrekte Funktionalität, das korrekte Performance, korrekte Interaktion an Schnittstellen und das Erkennen der Systemgrenzen/ODD-Grenzen verifiziert werden. Für die Ableitung konkreter Tests ist z.B. die Testmethode "Analyse von Szenarioräumen" anwendbar. Die Zerlegbarkeit der CORE-Szenarien (jedes Szenario, jede der 6 Schichten, jeder Parameter in jeder Schicht) sowie die Zerlegbarkeit der ADS-Funktionalitäten (Wirkketten) wird zu einer drastischen Reduktion der Anzahl der Testfälle genutzt.

Szenariobasierte Validierung

Die Validierung hat im Rahmen der VVM-Gesamtmethodik mehrere Aufgaben. Hierzu zählen unter anderem:

- die Überprüfung der Kundenakzeptanz und Usability,
- die Überprüfung der (Robustheit der) Konformität und operationalen Sicherheit des ADSystems im realen Betriebsumfeld zur Identifikation von Lücken in der Spezifikation sowie bei der Implementierung,
- die Überprüfung von Requirements, die weder durch Simulation oder Test auf Prüfständen oder Prüfgeländen verifiziert werden können,
- die Überprüfung des ODD-Metamodells (Unbekanntes) sowie Wissenszuwachs über die ODD (Bekanntes).

In der Validierung wird nachgewiesen, dass das ADS die Sicherheits- und Leistungsanforderungen auch unter stochastischen Bedingungen erfüllt, alle möglichen (Verkehrs-) Szenarien im realen Betriebsgebiet sicher beherrscht und ihre Implementierung von den Kunden akzeptiert wird. Darüber hinaus werden alle Merkmale von Szenarien getestet, die nicht in der Simulation oder auf dem Testgelände getestet werden können. Dazu gehört es z.B. nachzuweisen, dass die Grenzen

der ODD robust erkannt werden und eine Aktivierung des Systems nur innerhalb der ODD erfolgen kann. Die Überprüfung der Einhaltung von Verkehrs- oder Verhaltensregeln ist ein weiterer Schwerpunkt.

Die Validierung wird hier als szenarienbasierte Validierung bezeichnet, weil die gewählte Systematik zur Beschreibung / Modellierung der Szenarien in den Kategorien Menge der CORE Szenarien, erweiterte 6-Layer-Systematik, definierte Instanzen etc. die Test-Fail-Spezifikation steuern, Filter für die KPI zur Auswertung der Tests liefern und Organisationsstrukturen für die Ergebnisse und die Erweiterung des Wissens bzgl. der ODD sind. Szenarien stellen das zentrale Steuerungselement in der Validierung des ADS dar.

Zentrale Testinstanz sind laufleistungsbasierte Tests mit Dauerläufen oder Feldtests unter nicht-deterministischen bzw. stochastischen Bedingungen im realen Betriebssituationen und Zuständen im öffentlichen Straßenverkehr. Eine übergreifende Aufgabe ist die Identifikation von "unbekannten/Unbekannten" sowie von "unvollständigen Spezifikationen oder Implementierungen" (zur Adressierung der Verifikationslücke) und "unbeabsichtigtem Verhalten".

Aus den Felddaten werden mit Szenario-Filtern relevante Messdaten identifiziert, die das Ist-Verhalten des ADS im Szenario zeigen. Dies wird mit dem definierten Sollverhalten in dem Szenario abgeglichen. Abweichungen werden mit KPI (Key-Performance-Indicatore) evaluiert und anhand von Akzeptanzleveln bzw. falls vorhanden, anhand von spezifizierten Performance-Requirements bewertet.

Das ODD-Metamodel ist die Basis zur Identifikation von Abweichungen gegenüber den eingangs definierten systemunabhängigen Requirements für die Systementwicklung, den daraus abgeleiteten Anforderungen an das Verhalten und die Fähigkeiten des automatischen Fahrsystems, den Sollvorgaben im Requirement-Managements aber auch zur Vollständigkeit der Annahmen die im Entwicklungsprozess getroffen wurden. Hierzu zählt insbesondere die Validierung der Vollständigkeit des ODD-Metamodells selber. Das ODD-Metamodell wird als Datenfilter oder als Mittel zur Übertragung von Beobachtungen aus der realen Welt in dieses Modell zur Abdeckungsmessung oder Lückenidentifizierung verwendet. (siehe auch Kapitel 3.1.1.5 Realitätsabstraktion - Szenariobasiertes Testen)

Die Prüfung der Abdeckung der ODD durch die bisher durchgeführte Laufleistung bzw. Validierungstests und die Validierung der Vollständigkeit der ODD werden bei Feldtests oft parallel durchgeführt. Im Rahmen von Fahrzeug- und Feldtests muss die Abdeckung der definierten ODD in all ihren relevanten Dimensionen nachgewiesen werden. Darüber hinaus ist es erforderlich, noch unentdeckte Szenarioklassen oder relevante Domänenmerkmale zu identifizieren. In beiden Fällen wird das Metamodell als ein semantisches Modell der Domäne, in der die Ziel-ODD spezifiziert ist, und als ein Mittel zur Übertragung von Beobachtungen aus der realen Welt in dieses Modell benutzt. Dadurch kann sowohl die Abdeckung gemessen als auch Lücken entdeckt werden.

Validierungs-KPIs und Validierung ODD-Metamodell

Für die Validierung des ADS ist es notwendig, die Feldtest zu steuern. Die Menge der CORE-Szenario-Instanzen kann in diesem Fall zur Planung von Feldtest genutzt werden, etwa durch die Auswahl bestimmter Parameterklassen in denen schwerpunktmäßig Fahrten durchgeführt werden. Die Schwerpunktsetzung kann z.B. aus identifizierten Triggerbedingungen für risikobehaftete ungewollte Funktionsauslösungen oder auch aus dem Monitoring von Metriken zur

Risikoabschätzung einer Situation bestehen. Durch die Nutzung der Menge der CORE-Szenarien wird eine Kontrolle der Abdeckung des Testraumes möglich.

Ein Ziel der Systemvalidierung ist es, das Risiko von unbekannten auslösenden Ereignissen, die zu gefährlichen Situationen führen können, zu minimieren. Hierfür ist es notwendig, dass die im Rahmen der Feldtests durchgeführten Fahrten eine umfassende Abdeckung der in der ODD definierten Szenarien aufweisen. Um den Zielbetriebsbereich zu beschreiben, müssen die Feldtests so gesteuert werden, dass alle Bedingungen, die den spezifizierten Betriebsbedingungen und -zuständen entsprechen, hinreichend gut diskretisiert / gesamplet sind. Es ist außerdem erforderlich, eine statistisch relevante Anzahl von Fahrten durchzuführen, um noch nicht spezifizierte Situationen mit hinreichender Konfidenz erfassen zu können. Das ODD-Metamodell wird als Tool zur Kontrolle der Feldtests verwendet. Das ODD-Metamodell filtert Beobachtungen aus der realen Welt für Abdeckungsmessungen oder Lückenidentifizierung. Weitere Informationen dazu werden in Kapitel 3.1.1.5 Realitätsabstraktion - szenariobasiertes Testen ausgeführt.

Die Abdeckung der ODD wird durch die bisher durchgeführten Feldtests validiert. Das Ziel dieser Prüfung ist es, die Abdeckung des definierten Metamodells für die ODD in allen relevanten Dimensionen nachzuweisen und gleichzeitig alle unentdeckten/fehlenden Szenarioklassen oder relevanten Domäneneigenschaften zu identifizieren.
Bei der Validierung des ODD-Metamodells geht es darum sicherzustellen, dass durch ausreichend viele Fahrten keine neuen Szenarien oder Parameter gefunden werden, die für die o.g Validationsziel relevant sind. Dies ist eine zentral zu erbringende Evidenz, da es notwendig ist argumentieren zu können, dass das ODD-Metamodell die ODD hinreichend vollständig repräsentiert [51]. (siehe Kapitel 3.1.1.4.5.2 Szenarienabstraktion Grundlagen Vollständigkeitsargumerntation) In beiden Fällen wird die Szenariendatenbank als Teil des ODD-Metamodells als ein Tool verwendet, um Daten aus den Feldtest in der realen Betriebsumgebung zu sammeln und zu analysieren.

Bei den Feldtests im Rahmen der Validierung gehen die Prüfung der Abdeckung der ODD durch die bisher durchgeführte Laufleistung bzw. Validierungstests und die Validierung der Vollständigkeit der ODD werden bei Feldtests oft Hand in Hand. Dies hat ein Beobachtbarkeitsproblem zur Folge, es ist mit den Zielsensoren und Entscheidungsalgorithmen des automatisierten Fahrsystems nicht möglich noch nicht bekannte Szenarien oder auslösende Ereignisse direkt zu messen. Es ist eine geeignete redundante Messtechnik und Szenarioerkennung zu definieren. Das Vorhandensein von “unknown/uknown” kann dann indirekt abgeleitet und ggf. bestätigt werden.

Als geeignetere Prüfkriterien für die ODD-Abdeckung bieten sich der Prozentsatz der abgedeckten ODD-Szenarien bzw. Äquivalenzklassen oder die Anzahl der Fahrkilometer zwischen neu entdeckten ODD-Anforderungen an. Eine angemessene prozentuale Abdeckung der CORE-Szenarien und Parameterklassen sind relevante Testkriterien. Zur Steuerung des weiteren Testverlaufs wird die Zwischenbewertung der erreichten Testraum-Abdeckung herangezogen (siehe auch Kapitel 3.1.1.5 Realitätsabstraktion - Szenariobasiertes Testen).

Test-Endkriterium ist: Der feldbasierte Test hat eine relevante[1] Teilmenge der CORE Szenarioinstanzen aus dem Metamodell für die OOD abgedeckt und im Rahmen der Datenanalyse innerhalb der "Operational Safety & Conformity" wurden keine kritischen bzw. nicht akzeptablen Fehlern gefunden.

Szenariobasierte Evaluierung des Restrisikos

Die Evaluierung des aktuellen Risikolevels erfolgt für das in ein Fahrzeug integrierte ADS in der ODD - also auf der Systemebene durch szenariobasiertes Testen (Abbildung 38). Die Bewertung, ob das ermittelte Risiko akzeptabel oder nicht akzeptabel ist, basiert auf dem aus den TOP Safety Goal abgeleiteten Risikoakzeptanzkriterium. Im Rahmen von VVM wird als Akzeptanzkriterium beispielhaft die positive Risiko-Bilanz mit Fahrerleistungsreferenz verwendet. Das Kriterium ist in der zulässigen ODD für das integrierte ADS einzuhalten. Die Bestimmung des aktuellen Restrisikos erfolgt für definierte Klassen für Schwerekategorien von Schäden. Die Evaluierung wird in der Simulation durchgeführt und mit Tests auf Prüfgeländen oder im Feld gestützt bzw. validiert (Abbildung 38). Als Modell für die die Betriebssituationen und Zustände in der ODD wird das ODD-Metamodell verwendet.

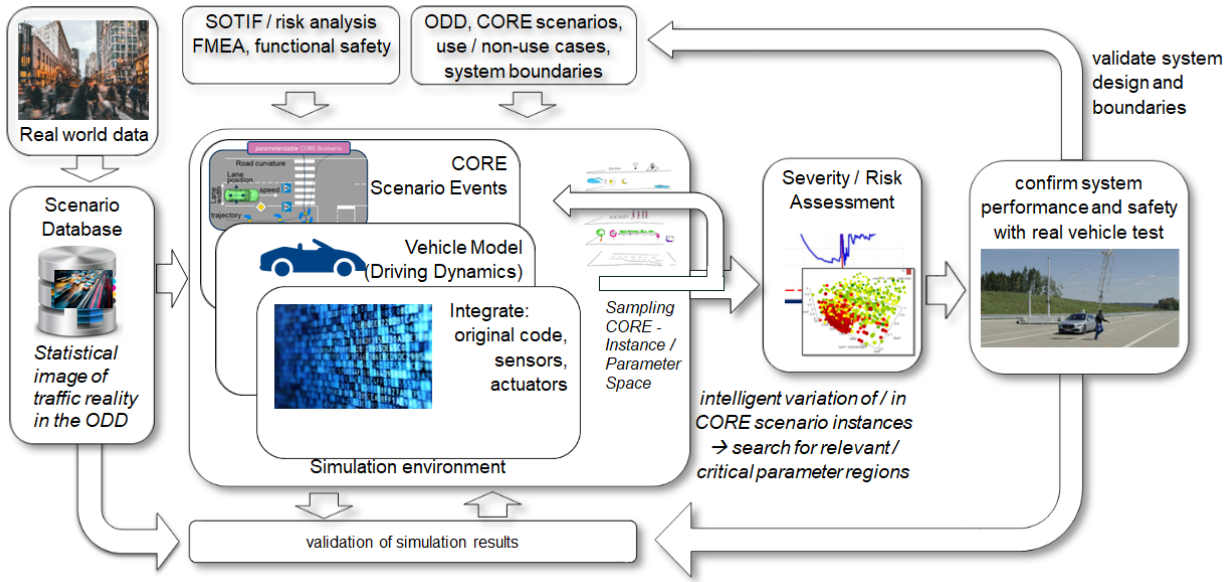


Abbildung 38: Beispielhaftes methodisches Vorgehen bei der szenariobasierten Evaluierung des Risikos (© Mercedes-Benz)

Für die Bewertung des Restrisikos werden die gleichen Risikoakzeptanzkriterien und Risikobewertungsfunktion wie im Risk Management Core verwendet. Dies ermöglicht zudem die durchgängige Verwendung von gleichen Risikomodellen, Evaluierungsfunktionen und Risikoakzeptanzlevel im gesamten Entwicklungsprozess (V-Modell). Als abgeleitetes Sicherheitsziel werden dann z. B. kollisionsrelevante Parametersätze bzw. deren Grenzen im zu untersuchenden Parameterraum der CORE-Szenarien identifiziert. Die Bewertung des Restrisikos des ADS im szenariobasierten Metamodell der ODD dient der abstrakten Darstellung der

[1] relevant aufgrund des Problems der Kontrollierbarkeit bei feldbasierten Tests, bei denen eine Reihe von konkreten Szenarien, die im ODD-Modell spezifiziert sind, extrem selten oder schwierig und gefährlich sein kann, im realen Straßenverkehr zu reproduzieren

Szenarioumgebung. Dies bedeutet, dass das Restrisiko für jedes CORE-Szenario in seinem Parameterraum bewertet wird. CORE-Szenarien sind zerlegbar in ein logisches Szenario, Beschreibungsebenen des Szenarios und die in der Ebene deklarierten Parameter.

Die Bewertung des Restrisikos erfolgt für jedes CORE-Szenario einzeln. Eine Möglichkeit ist es, den Parameterraum der CORE-Szenarioinstanzen mit einem intelligenten Suchalgorithmus zu durchsuchen, um die Risiko einer S0-S3-Kollision für das ADS zu bestimmen. Gestützt werden die Simulationen mit Felddaten wie insbesondere Sensordaten (FN, FP-Raten, etc.). Für die CORE-Szenarien erfolgt der Abgleich mit der Positiven-Risiko-Bilanz.

Mittels eines Fahrerleistungsmodells erfolgt eine Evaluierung der Fähigkeit eines menschlichen Fahrers der gewählten Äquivalenzklasse nicht kontrollierbare Szenarien des ADS zu kontrollieren. Dadurch wird gewährleistet, dass das System in der Lage ist, jedes Szenario statistisch mindestens ebenso gut zu beherrschen, wie ein (statistischer) menschlicher Referenzfahrer der gewählten Leistungsäquivalenzklasse.

Solche simulationsbasierten Evaluierungen werden verwendet, um die funktionale Korrektheit und die Einhaltung der Risikoakzeptanzkriterien beim Systembetrieb mit implementiertem Verhalten zu überprüfen.
Es wird geprüft, ob die Integration von Datenfusions-, Planungs- und Handlungsalgorithmen fähig ist, den Bereich konkreter (bekannter) Verkehrsszenarien korrekt und mit akzeptablem Risiko zu handhaben.
Es wird geprüft, ob die implementierten Algorithmen in den Systemkomponenten „Sense with Datafusion“, „Plan und Act“ in der Lage sind, die Bandbreite der (bekannten) konkreten Verkehrsszenarien korrekt und mit akzeptablem Risiko zu bewältigen. (siehe auch 3.1.1.5 Realitätsabstraktion - Szenariobasiertes Testen)

Die aus den Messungen gewonnenen KPIs werden ausgewertet und zur Validierung des Simulationsmodells verwendet. So kann die tatsächliche Leistungsfähigkeit z.B. des Sensorclusters abgeschätzt werden.
Auf diese Weise ist es möglich, Corner-Cases zu identifizieren, die zur Bestätigung der Simulationsergebnisse oder im Vorfeld zur Modellvalidierung durch Tests mit koordinierten Testobjekten (TST) auf dem Testgelände adressiert werden können (Kapitel 3.1.1.9 V&V Domäne).

Kriterien für das Testende

Die Testendekriterien im Feld des "Operational Safety & Conformity" bestehen aus verschiedenen Elementen.

Im Verifikationskonzept wurden Kriterien definiert, die beschreiben, wann die Verifikation akzeptabel (in Bezug auf sicher und kompliant) abgeschlossen ist, also die gegebenenfalls noch festgestellten Unterschiede zwischen spezifiziertem und implementiertem Verhalten akzeptabel sind.

Im Validierungskonzept wurden KPI´s definiert, die beschreiben, wann die Validierung akzeptabel abgeschlossen ist, also die gegebenenfalls noch festgestellten Abweichungen zwischen implementiertem und notwendigem Verhalten akzeptabel (sicher und kompliant) sind. Ferner sind die getroffenen Annahmen insbesondere das ODD-Metamodell und die Usability („Das richtige System wurde entwickelt“) zu belegen.

Bei der Evaluierung des Risikos ist zu belegen, dass das integrierte ADS mit dem implementierten Verhalten in Bezug auf das von ihn für Insassen und andere Verkehrsteilnehmer ausgehende Risiko unter dem akzeptablen Level (beispielhaft positive Risikobilanz mit Fahrer-Leistungsreferenz) ist. Hierbei sind auch Validierungs- und Verifikationsergebnisse zu nutzen.

Die VVM-Gesamtmethodik stellt sicher, dass das Sollverhalten des ADS und seine Architektur so gestaltet sind, dass systematische Bedrohungen und auslösende Ereignisse berücksichtigt werden. Die Auswahl der adressierten Sicherheitsmaßnahmen ist so, dass das Risiko auf ein akzeptables Niveau reduziert wird.

Das ODD-Metamodell wird in der realen Welt validiert, um sicherzustellen, dass das ODD-Metamodell, das im Design und in der V&V verwendet wird, eine gültige Darstellung der realen Ziel-ODD in Bezug auf die Menge der CORE-Szenarien und ihrer deklarierten Parameter ist. Dieser Schritt reduziert das "Unbekannte" im ODD-Metamodell. Der rekursive Ansatz in Design und V&V reduziert Gefahren oder gefährliche Situationen (siehe Abbildung 38).

Abbildung 39 zeigt die Ergänzungen des V-Modells (siehe auch Abbildung 27) durch die Kern-Elemente der VVM-Methode im Rahmen der Entwicklung des ADS. Sie liefern Evidenzen für eine Argumentation im Rahmen des ADS-Safety-Case, dass von dem ADS ein akzeptables Risiko für Fahrzeug, Insassen und andere beteiligte Verkehrsteilnehmer ausgeht.

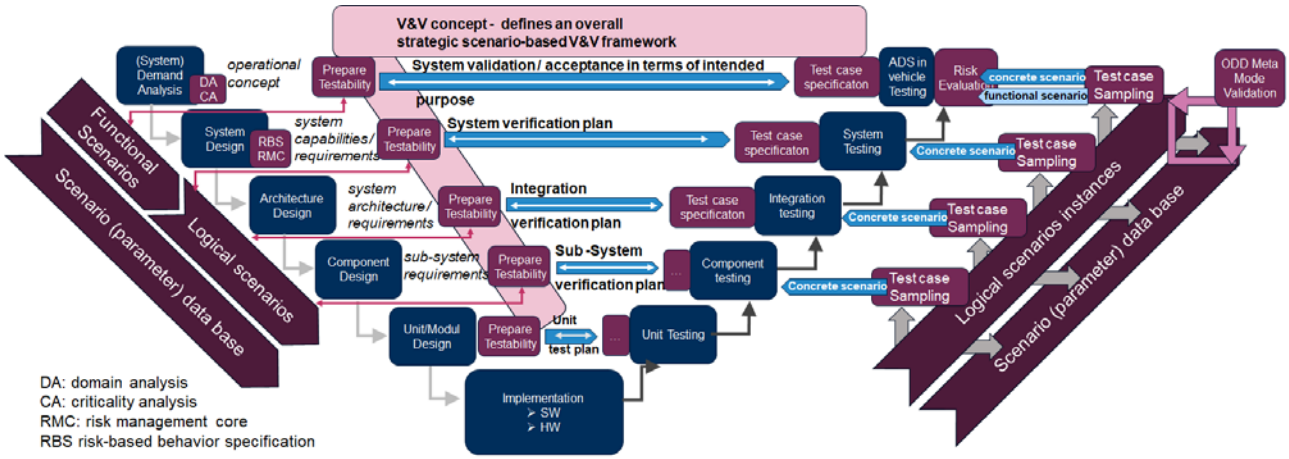


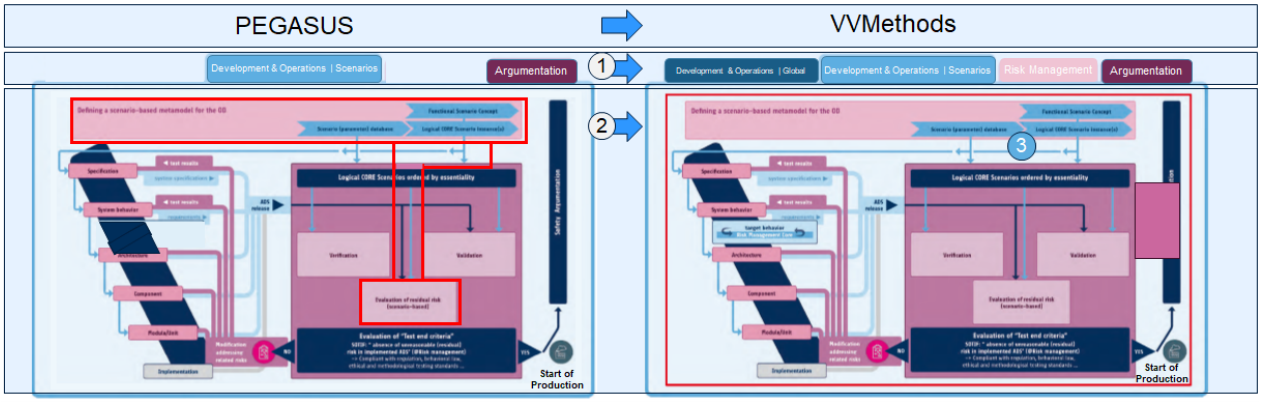
Abbildung 39: Ergänzungen des V-Modells durch Elemente der VVM-Gesamtmethode (in Rot)

Wo liegen die Unterschiede zwischen der Gesamtmethode PEGASUS und der Gesamtmethode VVM? Welcher Fortschritt wurde erzielt?

Die die im Rahmen dieses Berichtes vorgestellte VVM-Gesamtmethode ist eine Weiterentwicklung der PEGASUS - Gesamtmethode. In PEGASUS adressierte die Gesamtmethode die Fragestellungen “Wie sicher ist sicher genug?” und “Wie weise ich es nach?”. Dies führte zu einer Methode die insbesondere in der rechten Seite des V-Modells - also der Validierung und Verifikation - ansetzt und die unter anderem auf einem szenariobasierten Testen insbesondere im Rahmen der “Evaluierung des Restrisikos” in Verbindung mit einer Sicherheitsargumentation fußt. Detailliert wurden Szenarienkonzepte wie das 6-Ebenen-Modell und die Szenariendatenbank, die Absicherung von Parameterräumen von Szenarien sowie ein V&V-Konzept entwickelt, was ein koordiniertes V&V sowie den vernetzten Einsatz von unterschiedlichen Testinstanzen beschreibt. Unberücksichtigt blieben zum Beispiel Aspekte der Verifikation und Validierung eines konformen Verhaltens, ebenso der sich weiterentwickelnde Stand von Normen wie etwas ISO 21448 (SOTIF).

Im Gegensatz dazu adressiert die VVM-Gesamtmethode die weitergehende Fragestellung: “Welche Erweiterungen der von PEGASUS definierten Gesamtmethode sind erforderlich, um ein ADS zu entwickeln, das ein sicheres und konformes Verhalten aufweist und von dem kein unakzeptables Risiko für Fahrer, Insassen und andere Verkehrsteilnehmer bei einem Betrieb in seiner ODD ausgeht?”. Dies führte zu einem methodischen, prozessualen und organisationsspezifischen Vorgehen (inklusive seiner menschlichen, organisatorischen und technischen Aspekte) im Gesamtprozess “ADS-Entwicklung”, die insbesondere Evidenzen entlang des V-Modells erzeugt, die dies in einer Argumentation nachvollziehbar begründen.

In Abbildung 39 sind insbesondere die methodischen Unterschiede zwischen der PEGASUS und VVM Gesamtmethodik dargestellt.



(1) *GSN-based* argumentation	*Framework-based* Argumentation including *risk management*
(2) 6 Layer Scenario model, Set of Logical Scenarios & DB	6 Layer Model *& ODD Metamodel*
	Scenario-based specification of safe & compliant ADS behavior
	Scenario-based verification & validation
Scenario-based testing with *risk evaluation in V&V*	*Scenario-based* evaluation & management of risk level
use of test instances: simulation first, PG confirms simulation, endurance run assures stochastic aspects & complex situation	simulation first, PG confirms simulation, endurance run assures stochastic aspects & complex situation & validates Metamodel

Abbildung 40: Unterschiede zwischen der Gesamtmethode von PEGASUS (links) und VVM (rechts)

3.1.1.2.1 Die VVM - Sicherheitsargumentation

Die Herausforderung

Die Herausforderung einer Sicherheitsargumentation für ADS besteht darin, eine umfassende, explizite und nachvollziehbare Rechtfertigung für die Abwesenheit inakzeptabler Risiken im Betrieb zu gewährleisten. Außerdem müssen die Kombinationen aller möglichen Quellen von ADS-Risiken auf ganzheitliche Weise (Abbildung 41) beherrscht werden.

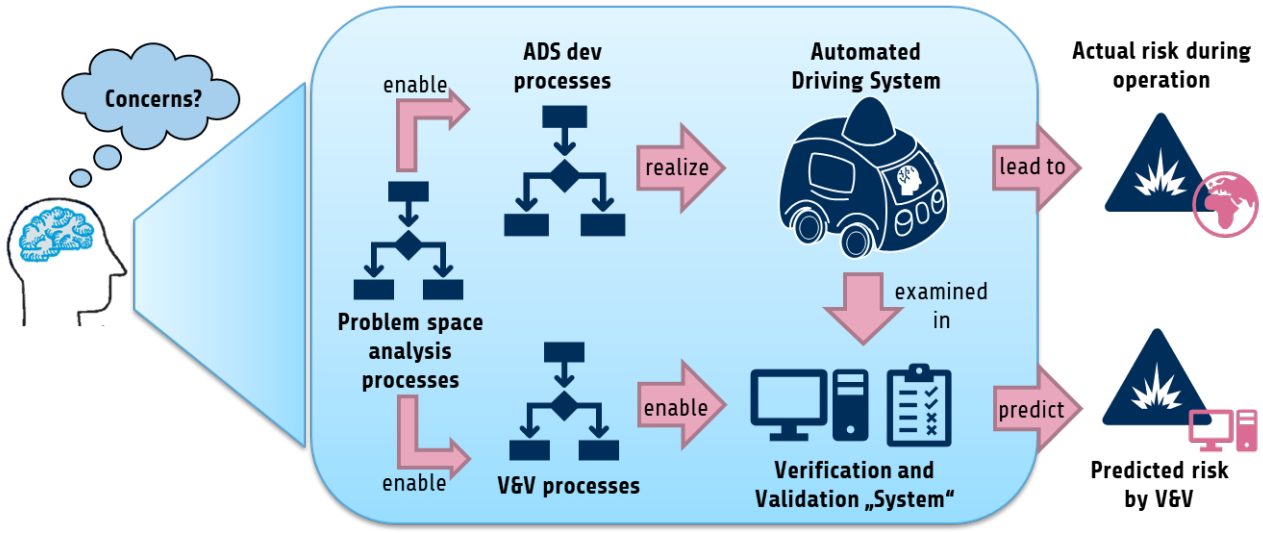


Abbildung 41: Überblick über die Quellen unzureichender ADS-Risikovorhersagen

Die Lösung

Die VVM-Sicherheitsargumentationsstruktur (Abbildung 42) stellt eine strukturierte Zerlegung der obersten Sicherheitsforderung „Abwesenheit inakzeptabler Risiken“ in umsetzbare Teilforderungen dar, die durch die in den VVM-Absicherungsprozessen erzeugten Nachweise gestützt werden können (siehe Kapitel 3.1.1.2.3). Was die Struktur besonders wertvoll macht, ist die explizite Beschreibung bewertbarer Strategien, die sich an der etablierten Praxis der Sicherheitsargumentation orientieren.

Hauptargumentationsstrategien

Auf oberster Ebene dient der Risk Management Core als Referenzmodell, um für die Übereinstimmung des geschätzten Risikos mit dem akzeptablen Risiko zu argumentieren. Des Weiteren wird ein szenariobasierter Ansatz als Referenzmodell gewählt, um die ADS-Performanz in der modellierten und in der realen Welt zu argumentieren. Die Komplexität des V&V-Systems hat erheblichen Einfluss auf die Validität der Risikoeinschätzung, weshalb die Performanz des V&V-Systems in einem separaten Zweig betrachtet wird. Genügend Vertrauen in die Gültigkeit der Nachweise für das Performanz-Argument wird erlangt durch die Absicherung der Problemraumanalysen, ADS-Entwicklungen und V&V-Prozessen. Analoge Muster werden genutzt für die Zerlegung des Prozessabsicherungszweiges unter Berücksichtigung der Spezifikation der erforderlichen Fähigkeiten sowie ihrer Entwicklung und Validierung unter kontrollierten und unkontrollierten realen Bedingungen (siehe Kapitel 3.1.1.2.2). Zusätzlich wird eine Kombination aus positiver und negativer Argumentation erbracht. Die positive Argumentation erbringt Nachweise für eine akzeptable Performanz des Systems und Angemessenheit der Prozesse (auch “Performance Assurance”, “Process Assurance”- Abbildung 42). Die negative Argumentation andererseits verfolgt das Ziel, Nachweise zu erbringen für die systematische Widerlegung objektiver und subjektiver Bedenken in Argumenten über Performanz und Prozesse (auch “Concern Management” - Abbildung 42).

Praktische Anwendungen:

Die VVM-Sicherheitsargumentationsstruktur strukturiert den Argumentationsbedarf für ADS-Risikovorhersagen auf der Basis von Annahmen über relevante Entwicklungs- und V&V-Artefakte

und hilft so, Deployment-Entscheidungen zu rechtfertigen. Des Weiteren bietet die Argumentation einen Ausgangspunkt für die Weiterentwicklung von Argumenten in konkreten ADS-Projekten unter Berücksichtigung unternehmensspezifischer Absicherungsmethoden und V&V-Systeme.

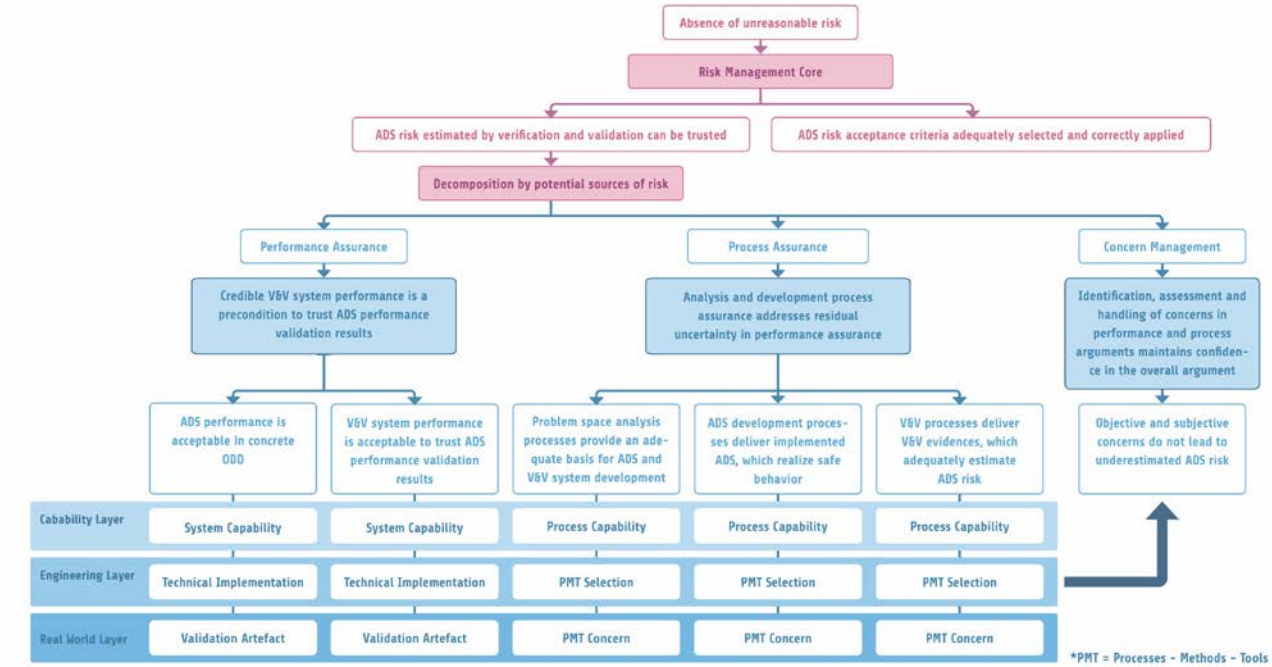


Abbildung 42: VVM-Sicherheitsargumentationsstruktur

3.1.1.2.2 Gesellschaftliche Erwartung und Erfüllung der Sicherheit

Hierzu hat VVM 3 Thesen erstellt:

- Für zunehmende Automatisierung rückt der Fokus der Sicherheit auf das Gesamtverhalten.
- Sicherheit wird durch das Fehlen eines unangemessenen Risikos definiert.
- ADS-Produkte sind sicher, weil sie die Erwartungen an die gesellschaftliche Sicherheit erfüllen. Daher definieren gesellschaftliche Interessengruppen Kriterien für die Risikoakzeptanz.

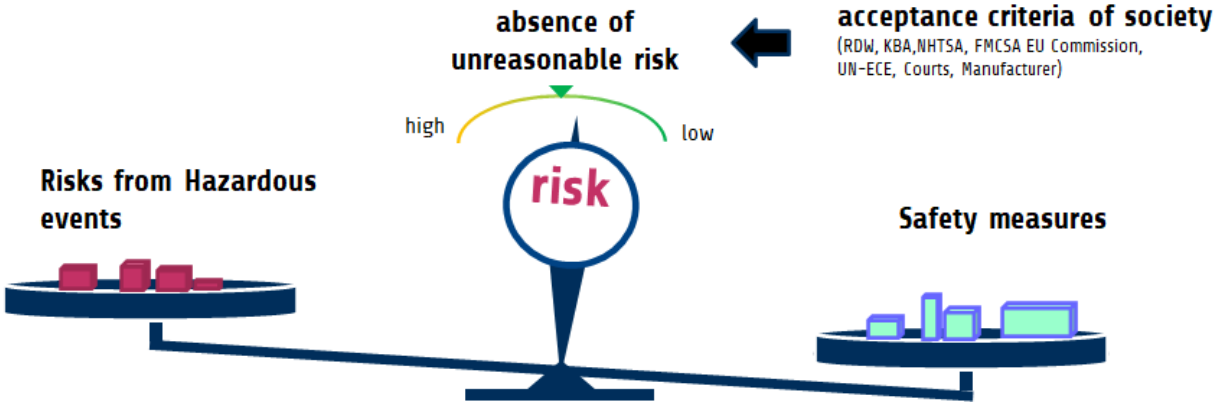


Abbildung 43: Verhältnis von Gefahren, Risiko, Sicherheitsmaßnahmen und Kriterien (© alle VVM.)

Die Analyse der Thesen führt zu folgenden Konsequenzen bzw. Schlussfolgerungen:

Schlussfolgerung #1: Eine ausreichende Risikomitigation inklusive Compliance muss der Gesellschaft erklärt werden.

> **Ansatz:** Eine regelbasierte systematische Top-Down-Argumentation, basierend auf dem Risikomanagement sowie auf Konzepten und Evidenzen von Entwicklung und Betrieb ermöglicht eine umfassende Erklärung.
>
> **Lösung:** Argumentation von sicherem Verhalten über ODD innerhalb des Absicherungs-Frameworks (Abbildung 42 nach unten).

Schlussfolgerung #2: Der Zusammenhang zwischen Risikoakzeptanzkriterien und Risiko durch gefährliche Ereignisse und Sicherheitsmaßnahmen muss modelliert werden.

> **Ansatz:** Explizite Risikomodellierung und Zuordnung auf Akzeptanzkriterien basierend auf Evidenzen von Entwicklung und Betrieb.
>
> **Lösung:** Durch die Perspektive des “Risiko-Managements” innerhalb des Absicherungs-Frameworks wird die notwendige Modellierung abgebildet (Abbildung 42 rechts oben).

Schlussfolgerung #3: Design und V&V und ODD-Metamodell müssen so strukturiert werden, dass alle notwendigen Evidenzen zur Risikomodellierung und Argumentation aus ihnen hervorgehen.

> **Ansatz:** Die Prozessstruktur von Entwicklung und Betrieb (Basis: V-Modell) einschließlich einer umfassenden Szenarien / Datenstrukturierung (z.B. ODD-Metamodell) müssen entlang des Risikomodells nach Verhalten und zugeordneten Fähigkeiten sowie der Argumentationsstrategie strukturiert werden, sodass diese die Schnittstellen der Risikomodellierung und Argumentation bezüglich Evidenzen bedienen.
>
> **Lösung:** Als geeignete Prüfkriterien für die ODD-Abdeckung bieten sich der Prozentsatz der abgedeckten ODD-Szenarien bzw. Äquivalenzklassen oder die Anzahl der Fahrkilometer zwischen neu entdeckten ODD-Anforderungen an Perspektiven “Development and Operation Global” und “Development and Operation scenario-based process extension” Szenarien innerhalb des Absicherungs-Framework (Abbildung 44 links).

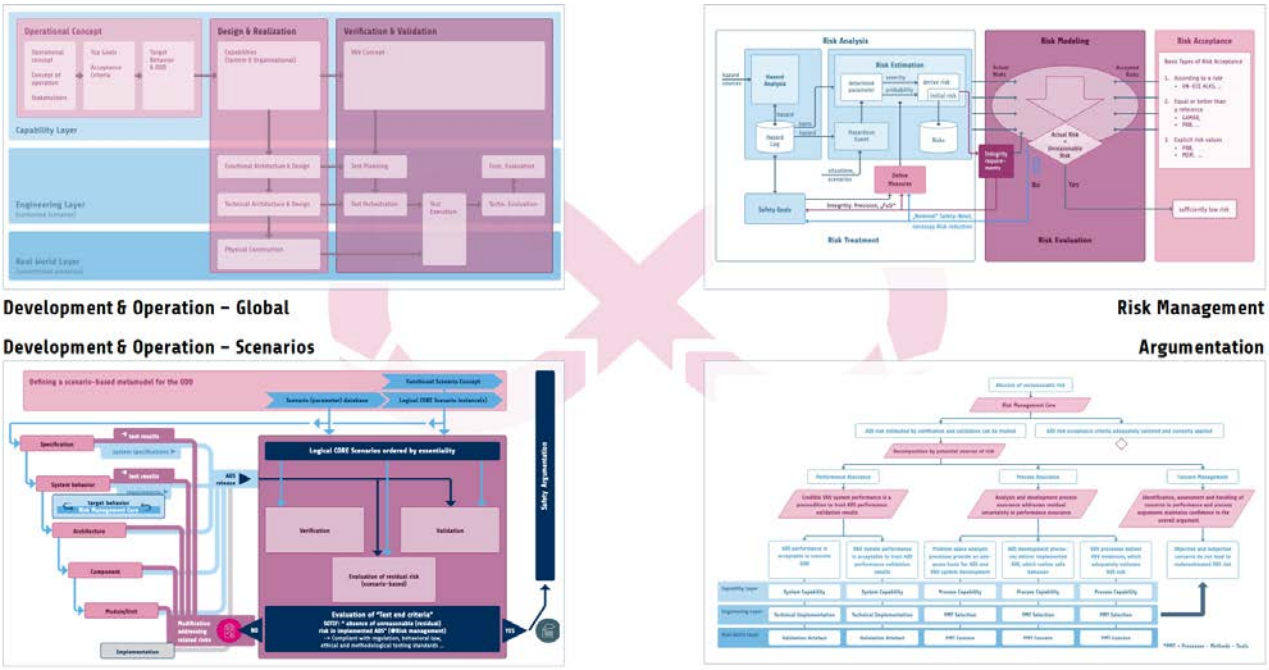


Abbildung 44: Absicherungs-Framework - alle vier Perspektiven des Meta Layers (© alle VVM)

Die o.g. Schlussfolgerungen und Lösungsansätze zeigen auf, dass sich die Argumentation hinsichtlich genutzter Evidenzen und Konzepte auf das Risikomanagement sowie auf die Entwicklungs- und Betriebsprozesse bezieht. Das Risikomanagement bezieht sich in gleicher Form wie die Argumentation auf die Entwicklungs- und Betriebsprozesse. Diese Relationen können als “Bottom up” Lieferung von Entwicklung und Betrieb betrachtet werden. Eine Top-Down-Steuerung der Entwicklungs- und Betriebsprozesse erfolgt über die Strategien der Argumentation und Maßnahmen/Anforderungen aus dem Risikomanagement.

Prinzipien zur Komplexitätsbeherrschung / Machbarkeit

Der o. g. Ansatz der 4 Perspektiven des Meta-Layers verfolgt das Ziel die starke Abhängigkeit des Lösungsraums von den vielfältigen Anforderungen zu strukturieren und einer iterativen und kontinuierlichen Entwicklung zugänglich zu machen. Folgende Voraussetzungen und Grundlagen wurden ermittelt:

- **Konsequente Zuordnung von Verantwortungen zu Perspektiven** bzw. Domänen oder Meta-Layer des Absicherungs-Frameworks und deren nahtloses Zusammenspiel. Dies bedeutet z.B., dass eine Risikobewertung einer Maßnahme immer im Risikomanagement abgebildet werden soll.

- **Reproduzierbarkeit der Elemente des Absicherungs-Frameworks** in Bezug auf die Argumentation. Dies bedeutet, dass innerhalb eines Flusses bzw. einer Kette von Elementen des Entwicklungsflusses jede Darstellung der Elemente die Anforderungen der vorherigen Darstellung wiedergibt. Mit anderen Worten: Eine Kette von Repräsentation des Systems muss so aufgebaut sein, dass jede Repräsentation die Anforderungen der vorhergehenden vereinigt. So wird eine “Explosion von Argumentationspfaden" vermieden (siehe Abbildung 45).

- **Die Verwendung von Metriken**, die die Eigenschaften zwischen den Repräsentationen des Systems (Elementen des Frameworks) transferieren können, ermöglicht die

Rückverfolgbarkeit der Elementeigenschaften. Der harmonisierte Umgang mit den Metriken ist daher ebenso wesentlich für den Top-Down und Bottom up Prozesse zwischen den Perspektiven (siehe Abbildung 45).

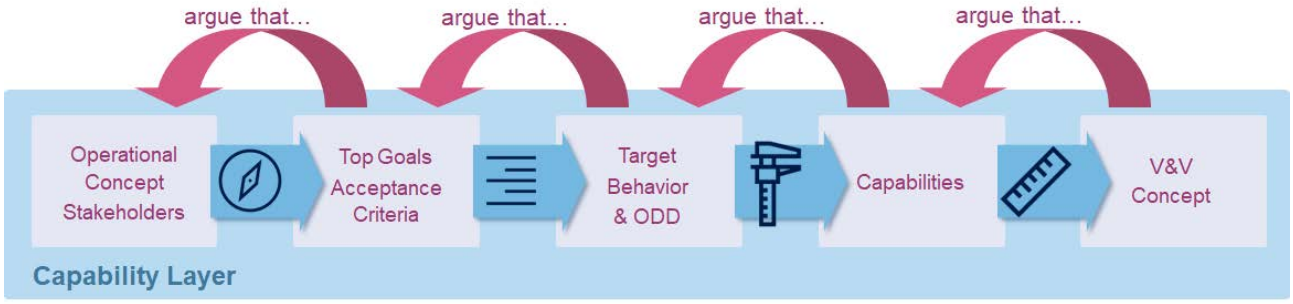


Abbildung 45: Beispiel für eine argumentative Reproduzierbarkeit der Elemente des Frameworks und der Metriken die deren Eigenschaften transferieren

3.1.1.2.3 Hauptkonzept für die Absicherung des Sicherheitsanspruches

Das zentrale Argument wird durch den Nachweis sicheren Verhaltens innerhalb der ODD durch eine Argumentation bestimmt. Die Hauptsystematik besteht darin, "verhaltenssichere" ODD-Bereiche durch Extrapolation (Abbildung 46 links) zu erweitern, die sich auf V&V-Beweise/Nachweise (Abbildung 46 rechts) beziehen.

Ansatz zur Extrapolation "sicherer Verhaltensbereiche"

- Auswahl risikosensitiver Bereiche des Verhaltens durch Zerlegung von ODD und Design entlang des Risikomodells.
- Erstellung von Extrapolationsmodellen für sicheres Verhalten und Definition von Risiko- und Performance-Schwellen entlang des Risikomodells.

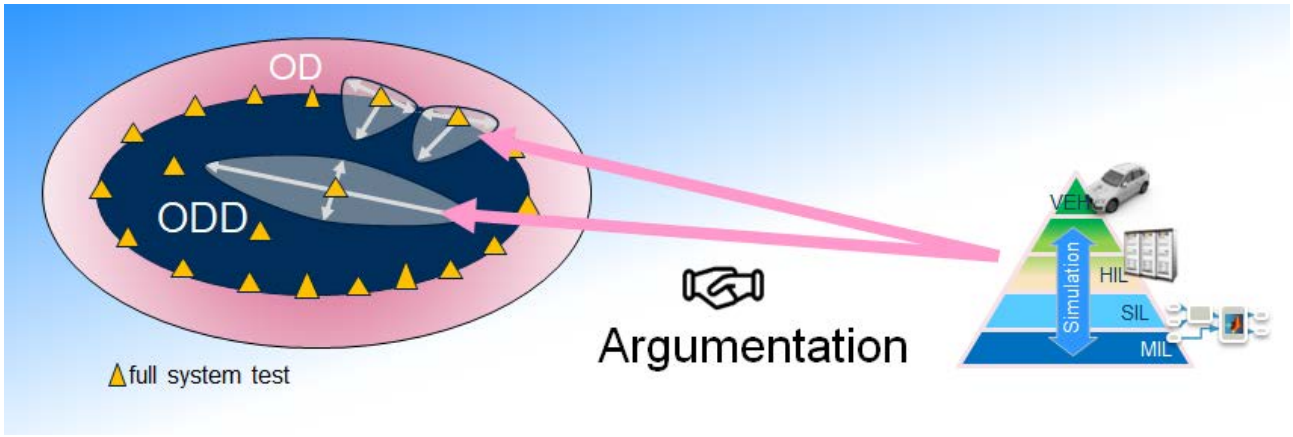


Abbildung 46: Hauptidee: Sicherung des Speicherverhaltens bei ODD (© VVM)

Die Argumentation der Absicherung wird als wesentlicher Befähiger für ein nachvollziehbares Herunterbrechen gesellschaftlicher Ansprüche und damit für erklärbare Compliance angesehen, um im Wesentlichen Fahrzeuge in Verkehr zu bringen.

Die Hauptidee der Argumentation ist es, über verschiedene Perspektiven des Verhaltens zu argumentieren (erforderliches, spezifiziertes und reales Verhalten). Ziel ist es, systematisch Lücken zwischen diesen Perspektiven zu identifizieren (Abbildung 47 links). Da sich die

Argumentation im Wesentlichen nur auf Nachweise des Entwicklungsprozesses stützen kann, sollten die Perspektiven des Verhaltens im Rahmen der Entwicklung dargestellt werden. Dies wird durch drei Schichten (Layer) in den Meta Layern für Entwicklung und Betrieb, entsprechend den Perspektiven (Abbildung 47) hergestellt. Die horizontalen Ebenen stellen Entwicklungs- und Betriebsarten dar, die die vertikalen Bereiche Design und Verifikation und Validierung definieren.

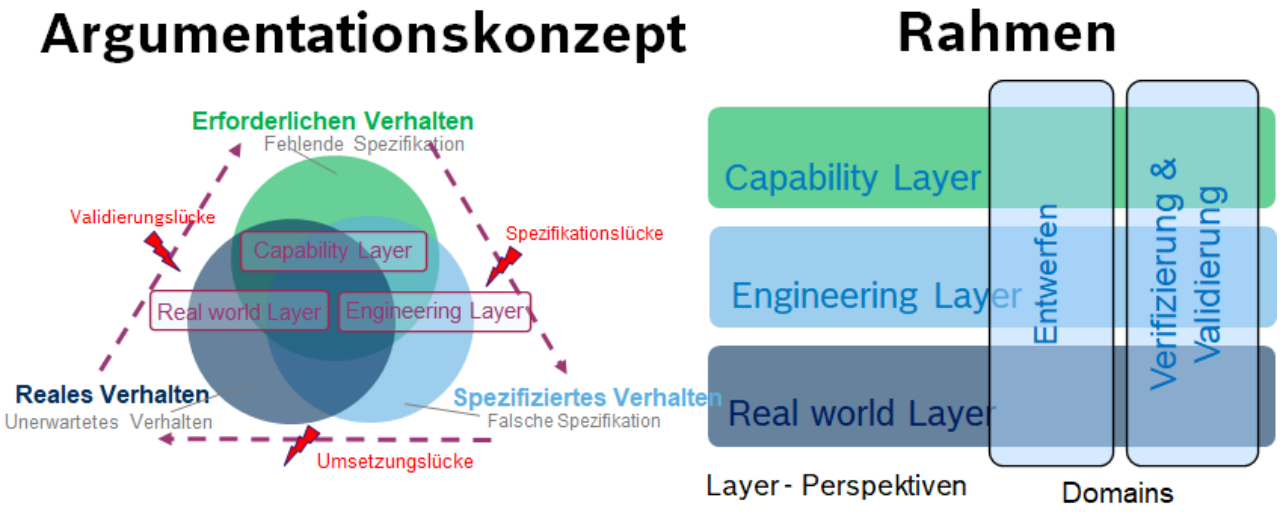


Abbildung 47: links: Validierungsdreieck [52], rechts Assoziation von Argumentationskonzept und Schichten von Entwicklungsrahmen (© VVM)

Übersicht 3-Ebenenmodell:

- **Fähigkeiten Layer: Komposition abstrakter Anforderungen** - relevante gesellschaftliche Ansprüche als Gesetze/Standards & Marktversprechen werden in das "erforderliche Verhalten" und die damit verbundenen Fähigkeiten einschließlich V&V-Fähigkeiten übertragen.
- **Engineering Layer: Systemspezifikation durch Zerlegung der abstrakten Anforderungen** führt zur Spezifikation des Verhaltens durch das Design und dessen Nachweis durch Verifikation in einer kontrollierten Umgebung.
- **Real World Layer: Interaktion des physischen Systems mit der unkontrollierten Umgebung** ermöglicht die Validierung von Verhalten mit Fokus auf Resilienz im offenen Kontext über den gesamten Lebenszyklus.

Zusammenspiel von Entwicklung und Argumentation

Die Ziele der Entwicklung wie z. B. Freigabe von Fahrzeugen und andere Ziele sollten den Argumentationsansprüchen entsprechen. Die Argumentationsstrategie beruht auf den Konzepten von Design und V&V und der Risikomodellierung, umgekehrt liefert die Argumentation Regeln, um präzise geeignete Beweise zu formen (Abbildung 48).

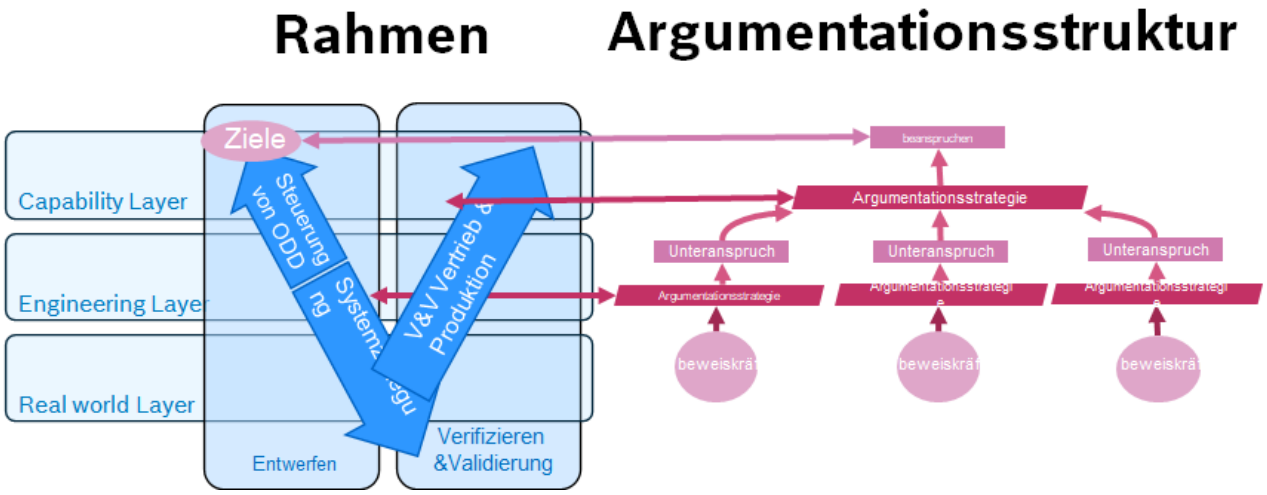


Abbildung 48: Assoziation von Entwicklungsstruktur und Argumentationsstruktur (© VVM)

Warum einen Capability Layer einrichten?

Komplexität kann durch Abstraktion beherrscht werden.

- Die Abdeckung von sicherem Verhalten in den Bereichen der ODD kann - einschließlich Sicherheitsbedenken - über Fähigkeiten argumentiert werden. Hintergrund dafür ist der universelle Charakter der Fähigkeiten, der Ihre Bedeutung für sicheres Verhalten über spezifische ODD-Bereiche abschätzbar macht. Gleichzeitig eignen sich Fähigkeiten auch dazu, technische Systemumfänge zu bewerten. Die Eigenschaft der Fähigkeiten, technische Systemumfänge und Verhaltenssicherheit über ODD-Bereiche zu verbinden beschreibt im Kern die Art und Weise der hier angewandten Komplexitätsbeherrschung durch Fähigkeiten. Darüber hinaus können Fähigkeiten über Systemanforderungen rückverfolgbar zerlegt werden, und somit können auch Verifikation und in Teilen auch die Validierung konsistent zerlegt werden.
- Der universelle Charakter einer Verhaltensbeschreibung ermöglicht es, die Parallelität und Überlappung funktionaler Beschreibungen zu bündeln und damit eine Bewertbarkeit hinsichtlich der für das Verhalten notwendigen Fähigkeiten herzustellen. Damit dient die abstrakte Verhaltensbeschreibung ebenso der Abdeckung von sicherem Verhalten in den Bereichen der ODD. Zudem ermöglicht es eine Sicherheitsargumentation auf abstrakter Verhaltensebene einen Anspruch, der sich auf Sicherheitsakzeptanzkriterien bezieht, z. B. eine positive Risikobilanz mit Hauptreferenz auf der Grundlage der Unfallstatistik zu argumentieren damit die Verbindung zur Gesetzten und Normen herzustellen.

Zusammenfassung

Die Absicherungs-Argumentation ermöglicht eine konsistente und nachvollziehbare Zerlegung von Ansprüchen bis hin zu Verifikation & Validierung, wodurch erklärbare Compliance für die Freigabe von Fahrzeugen in den Verkehr ermöglicht wird.

Design und V&V müssen die Argumentation mit Nachweisen unterstützen. Daher ist ein nahtloses Zusammenspiel zwischen Argumentation und Design und V&V, idealerweise konform zu relevanten Industriestandards, notwendig. Eine Lösung für diese Herausforderung ist das Absicherung-Framework.

3.1.1.2.4 Sicherheitsargumentation

Innerhalb der Top-Level-Argumentation gibt es mehrere Argumentationsstrategien und Evidenz, die sich auf eine durchgängige Verhaltensspezifikation stützen. Methoden und Modelle zur Umsetzung einer solchen Spezifikation automatisierter Fahrsysteme (ADS) sind demnach wichtige Beiträge von VVMethoden. Aus einer argumentativen Perspektive können diese Beiträge unterteilt werden in die Argumentation zur Leistungsfähigkeit eines ADS (ADS Performance Assurance) und die Argumentation zu den Prozessen für die Entwicklung und Absicherung (Process Assurance) (siehe Abbildung 49).

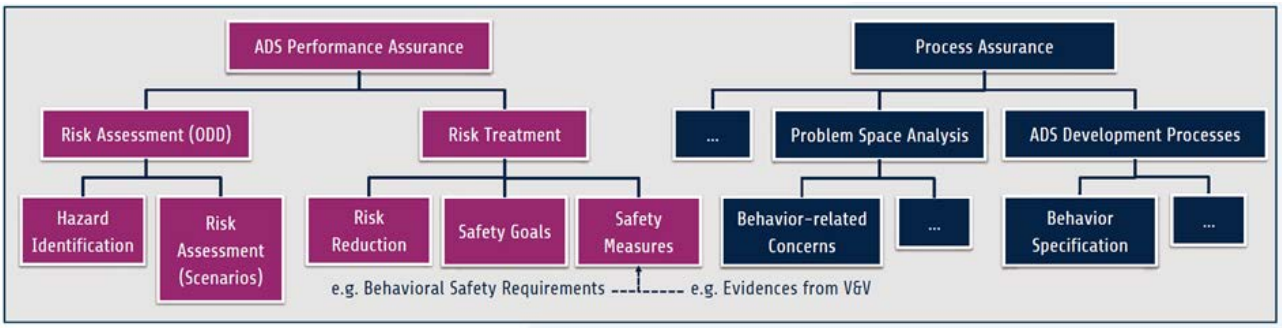


Abbildung 49: Vereinfachte Übersicht der argumentativen Beiträge einer Verhaltensspezifikation zur Top-Level-Argumentation

3.1.1.2.4.1 ADS Performance Assurance

Behauptung: Das ADS weist die erforderlichen Systemfähigkeiten auf, so dass es kein unangemessenes Risiko in seiner Operational Design Domain (ODD) von ihm ausgeht.

Um diese Behauptung zu untermauern, argumentieren wir, dass einerseits das unangemessene Risiko in der ODD definiert sein muss. Andererseits müssen Sicherheitsmaßnahmen spezifiziert, implementiert, verifiziert und validiert werden, die ein unzumutbares Risiko verhindern.

3.1.1.2.4.1.1 Risikobewertung

Behauptung: Unangemessenes Risiko ist für die Operational Design Domain definiert.

Um zu argumentieren, dass ein unangemessenes Risiko für die ODD definiert ist, muss eine Risikobewertung durchgeführt werden. Gefährliche Ereignisse werden in bekannten Szenarien identifiziert und ihr Risiko wird analysiert. Eine explizite Verhaltensspezifikation unterstützt eine systematische Identifikation von gefährlichen Ereignissen, da sie Kontextelemente kausal mit spezifizierten Manöveroptionen verknüpft. Diese Spezifikation wird in VVMethoden verwendet, um gefährliches Verhalten zu identifizieren, das zu gefährlichen Ereignissen führen kann. Da die Risikoanalyse auf bekannte Szenarien beschränkt ist, sind weitere Beweise erforderlich, die zeigen, warum das geschätzte Restrisiko für unbekannte Szenarien als akzeptabel eingeschätzt wird.

3.1.1.2.4.1.2 Risikobehandlung

Behauptung: Die Verhaltenssicherheitsanforderungen werden durch das automatisierte Fahrsystem erfüllt.

Auf Grundlage der in der Operational Design Domain bewerteten Risiken werden Sicherheitsziele definiert, die die notwendige Risikominderung und Sicherheitsintegrität der spezifizierten

Sicherheitsmaßnahmen beschreiben. Sicherheitsmaßnahmen werden für mehrere Geltungsbereiche spezifiziert. Zum Beispiel beschreibt die ISO 26262 wie funktionale und technische Sicherheitsanforderungen für einen bestimmten Entwicklungsgegenstand spezifiziert werden können. Da das Sollverhalten spezifiziert wird, ohne einen bestimmten Entwicklungsgegenstand vorauszusetzen, führt VVMethoden Verhaltenssicherheitsanforderungen ein, welche Sicherheitsmaßnahmen in Bezug auf das Sollverhalten in den betrachteten Szenarien spezifizieren. Solche Anforderungen ermöglichen eine explizite Darstellung kontextabhängiger Risiken und unterstützen eine transparentere Kommunikation.

Wir argumentieren, dass kein unangemessenes Risiko vom automatisierten Fahrsystem in der ODD ausgeht, wenn es die Verhaltenssicherheitsanforderungen erfüllt. Die Evidenzen werden durch V&V-Ergebnisse erbracht, die zeigen, dass das ADS die Sicherheitsanforderungen erfüllt.

3.1.1.2.4.2 Process Assurance

Weitere Beiträge einer durchgängigen Verhaltensspezifikation werden bei der Analyse des Problemraums erbracht. In diesem Zweig der Argumentation liegt der Fokus auf der Erhebung von Stakeholder-Bedürfnissen (z.B. im Hinblick auf das Verhalten eines ADS im Straßenverkehr). Diese Bedürfnisse werden explizit in den Prozess der Verhaltensspezifikation integriert.

Behauptung: Der Entwicklungsprozess stellt die Analyse verhaltensbezogener Bedürfnisse sicher.

Behauptung: Der Entwicklungsprozess legt der Spezifikation des Sollverhaltens Stakeholder-Bedürfnisse zugrunde.

3.1.1.2.5 Herausforderung Sicherheit-Management automatisierter Fahrsysteme

Grundsätzlich erfordert die Homologation von AD-Systemen die Erfüllung gesellschaftlicher Sicherheitserwartungen. Bei AD-Systemen sind in der Regel mehrere Gefährdungen gleichzeitig vorhanden, die aus verschiedenen Quellen wie z. B. Normen, Verhalten, Technologie identifiziert werden können.

Lösung: Risk-Management-Core (RMC)

Der Risk Management Core stellt einen iterativen Prozess dar, der das tatsächliche Risiko mit dem akzeptierten Risiko in Einklang bringt. Der RMC unterstützt eine explizite Darstellung und Behandlung von Risiken:

- Risiko als führendes Maß für Sicherheit.
- Aggregation aller Systemrisikoaspekte über den "Risk-Modelling"-Ansatz.
- Iterative Anpassung des Systemrisikos an Risikoakzeptanzkriterien.

Inputs für den Risk Management Core (RMC)

- Gefährdungen
- Situationen / Szenarien
- Risikoakzeptanzkriterien

Outputs des Risk Management Core (RMC)

- Sicherheitsziele
- Risikobasierte Entscheidungen
- Risikominderungsmaßnahmen in Zusammenhang mit Zielwerten
- Aggregierte Risikoaspekte für die Sicherheitsargumentation

Die Outputs erfüllen aktuelle Anforderungen aus Normen und unterstützen industrielle Engineering-Prozesse.

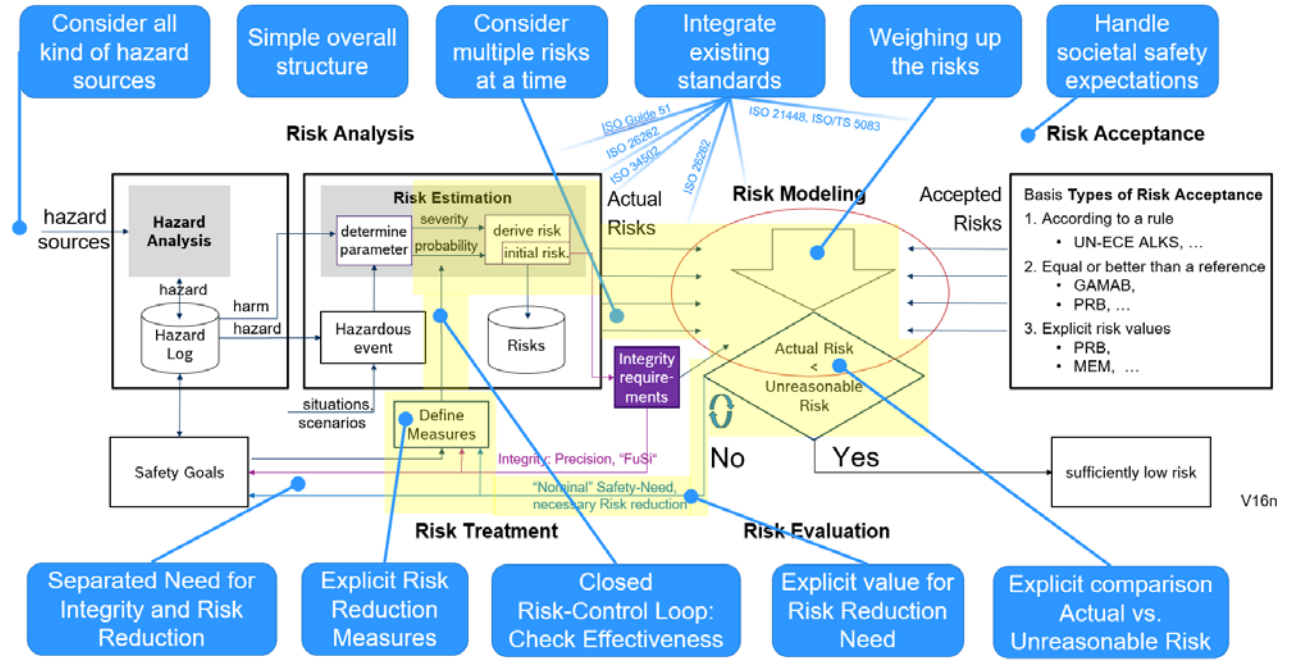


Abbildung 50: Eigenschaften des “Risk Management Core” (RMC)

Schnittstelle zur Sicherheitsargumentation

Der RMC unterstützt Argumente

- für Risiken denen konkrete Werte zugeordnet sind,
- dass Risikoakzeptanzkriterien gut ausgewählt und ausreichend berücksichtigt werden,
- für ausreichend risikomindernde Maßnahmen,
- die zeigen, dass das Restrisiko ausreichend niedrig ist und
- warum Risiken und Akzeptanzkriterien kombiniert werden können.

Anwendung für mehrere Zwecke

Der RMC erfasst alle Gefährdungen und Sicherheitsziele des gesamten Produkts. Gleichzeitig wird er für weitere verschiedene dedizierte Aufgaben angewendet:

- Erstellung eines sicheren Sollverhaltens,

- Ausrichtung von Systemrisiken an Akzeptanzkriterien,
- Risikoabschätzung spezifischer Elemente,
- Risikobewertung zu Beginn der Produktion (SOP).

3.1.1.2.6 Strategischer Link zwischen Test & Absicherung und der Sicherheitsargumentation

Wie zuvor in der Top-Level Argumentation besprochen, unterscheidet die Sicherheitsargumentation zwischen Performance- und Prozessabsicherung bei den Risikoquellen. In Bezug auf V&V-Aktivitäten und -Ergebnisse wurde hier eine neue Klassifizierung eingeführt, um explizit zwischen der Performance des AD-System und des V&V-System zu unterscheiden und die gestiegene Komplexität von V&V-Aktivitäten und der Testinfrastruktur für automatische Fahrsysteme nach SAE Level 3 und höher zu berücksichtigen.

In der Performanceabsicherung des AD-Systems findet sich die klassische Ansicht aggregierter Testergebnisse zur Unterstützung höherer Leistungsanforderungen. Abbildung 51 veranschaulicht ein Beispiel dafür, wie die Argumentation einer Wahrnehmungsfähigkeit eines Fußgängerüberwegs bis hin zu den Validierungsartefakten strukturiert werden kann. Diese strukturierten Argumente sind darauf ausgelegt zu argumentieren, dass das System in diversen Szenarien konsistent wie erwartet funktioniert. Die Schlüsselrolle der Argumentation besteht darin, die Begründung für die Verbindung spezifischer Performanceanforderungen mit relevanten Tests mithilfe dedizierter Prozesse bereitzustellen, während Prozesse selbst, z.B. wie man Testergebnisse effizient aggregiert, hier nicht entwickelt werden.

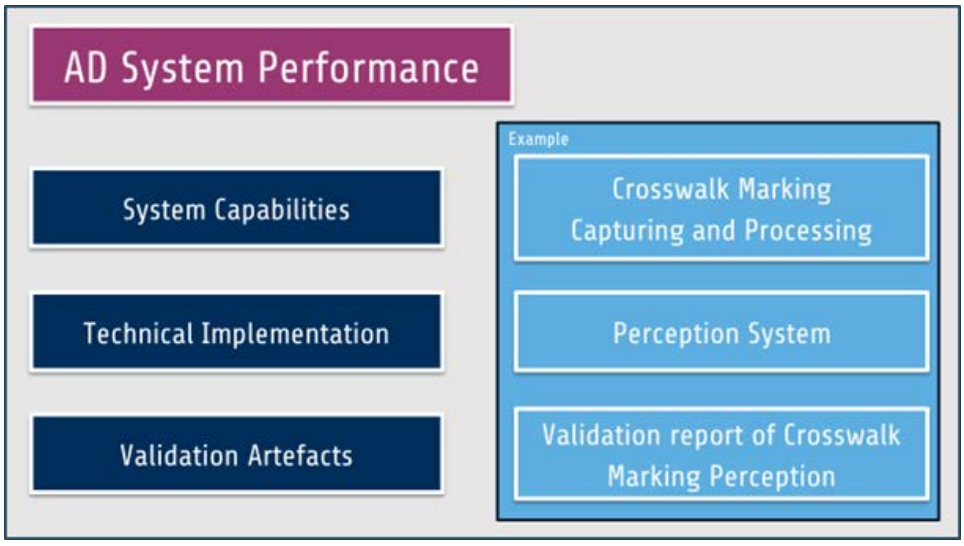


Abbildung 51: Argumentation angewendet auf die Absicherung der ADS-Fähigkeiten

Durch die explizite Einbeziehung der Performanceabsicherung des V&V-System wird der Komplexität aller relevanten Testumgebungen, die als V&V-System bezeichnet werden, Rechnung getragen. Abbildung 52 dient als anschauliches Beispiel und zeigt die generische Argumentationsstruktur an einem Beispiel einer virtuellen Testumgebung. Dies hebt den intrinsischen Wert der SetLevel-Projektergebnisse innerhalb der breiteren VVM-Argumentation hervor. Eine explizite Argumentation der V&V-Systemleistung stärkt die gesamte Sicherheitsargumentation und bietet einen expliziten Zweig, in dem zum Beispiel Zuverlässigkeitsartefakte als Evidenzen argumentiert werden.

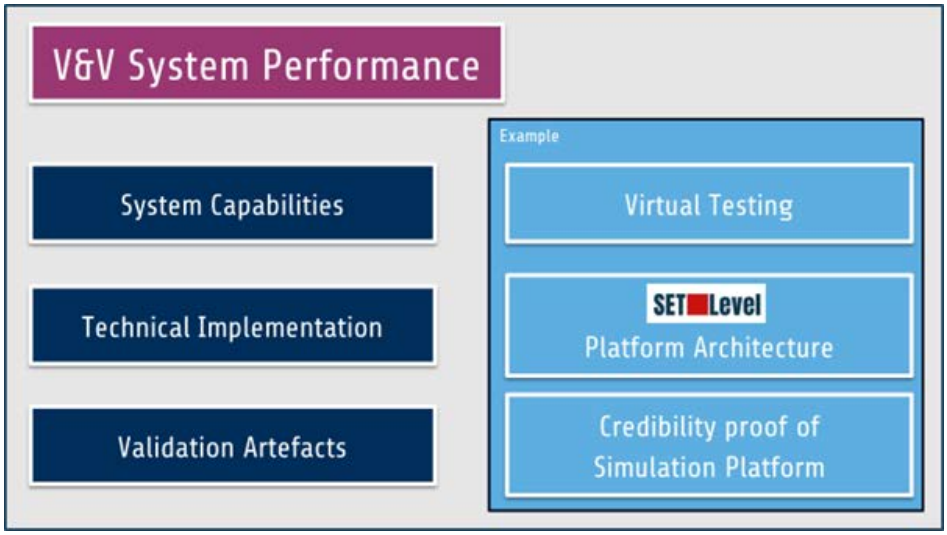


Abbildung 52:Argumentation angewendet auf die Zuverlässigkeit der Fähigkeiten des V&V Systems

Die Prozessabsicherung argumentiert, warum bestimmte Prozesse zur Entwicklung eines glaubwürdigen V&V-Systems führen und die Evidenzen bereitstellen, um die AD-Systemleistung zu gewährleisten. Ausgewählte Prozesse, Methoden und Werkzeuge sind in spezifischen erforderlichen Fähigkeiten verwurzelt, grenzen ihren wahren Zweck ab und stimmen sie mit dem Ziel der Adressierung von Bedenken ab. Ein Beispiel wird in Abbildung 53 für den Testplanungsprozess gezeigt. Eine Fortsetzung auf diese Weise führt zu einer verständlichen Prozessabsicherung für die Entwicklung des V&V-Systems.

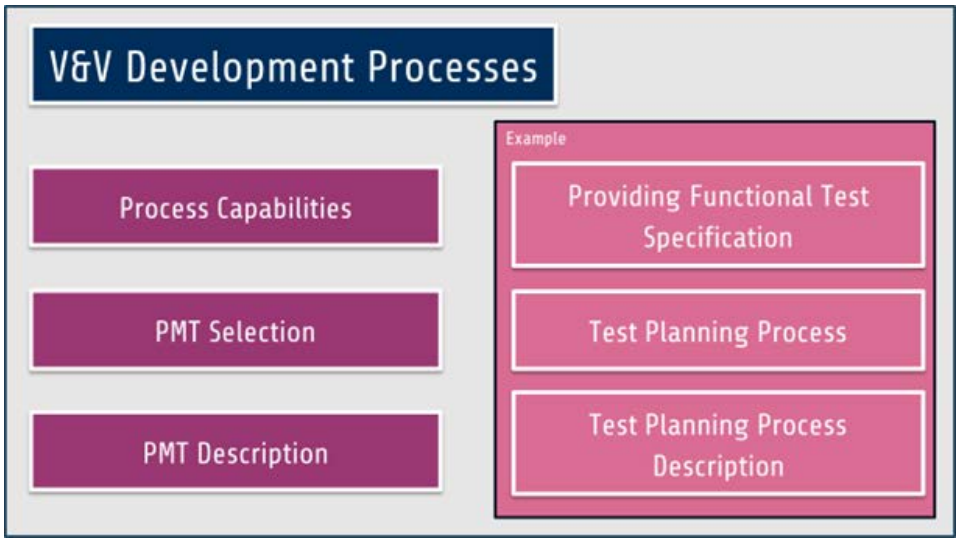


Abbildung 53: Prozessabsicherung für die Erstellung der funktionalen Testspezifikation

Im Detail wurde die nächste Ebene der Sicherheitsargumentation für die Prozesse zur Erstellung des V&V Systems in GSN-Form ausformuliert. Die mit „G“ referenzierten Elemente sind die Ziele (Goals) der Argumentation. Dieses Ziel kann sich auf einen Kontext (Context) „C“ beziehen. Die Argumentation wird zusätzlich durch eine Argumentationsstrategie (Strategy) „S“ unterstützt. In Abbildung 54 wird diese Form für die Dekomposition des Ziels „V&V Prozesse liefern V&V Evidenzen, die das Risiko des ADS hinreichend abschätzen“ genutzt. Die Liste der Evidenzen dient hier als Kontextreferenz und wird im Perfomance-Zweig erzeugt. Die zugrundeliegende

Strategie ist die Dekomposition in vier Unterprozesse, dem Erstellen des V&V Konzeptes, der Ableitung der Verifikations- und Validierungsaufgaben, und die Ableitung und der Realisierung aller relevanten Tests aus den V&V Aufgaben. Im V&V Konzept ist der besondere Zusatz der Pre- und Post-Deployment Strategie zu beachten, denn die Sicherheit muss auch nach dem In-Verkehr-Bringen nachgewiesen werden.

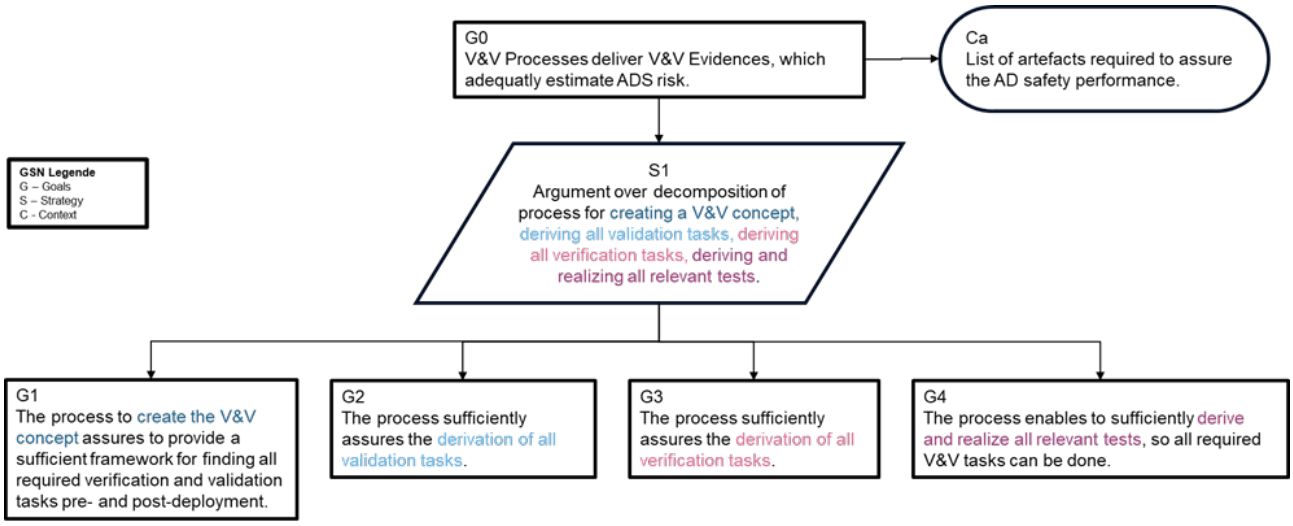


Abbildung 54: GSN für die Dekomposition der Prozessabsicherung zur Entwicklung des V&V Systems

Die nächste detaillierte Argumentationsstrategie ist in Abbildung 55 zu sehen und beschreibt die Dekomposition des Ziels zur Ableitung und Realisierung aller relevanten Tests aus den V&V Aufgaben. Dieses Ziel wird in die folgenden vier Unterziele dekomponiert, der Testplanung, der Testorchestrierung, der Testdurchführung und der Testevaluation.

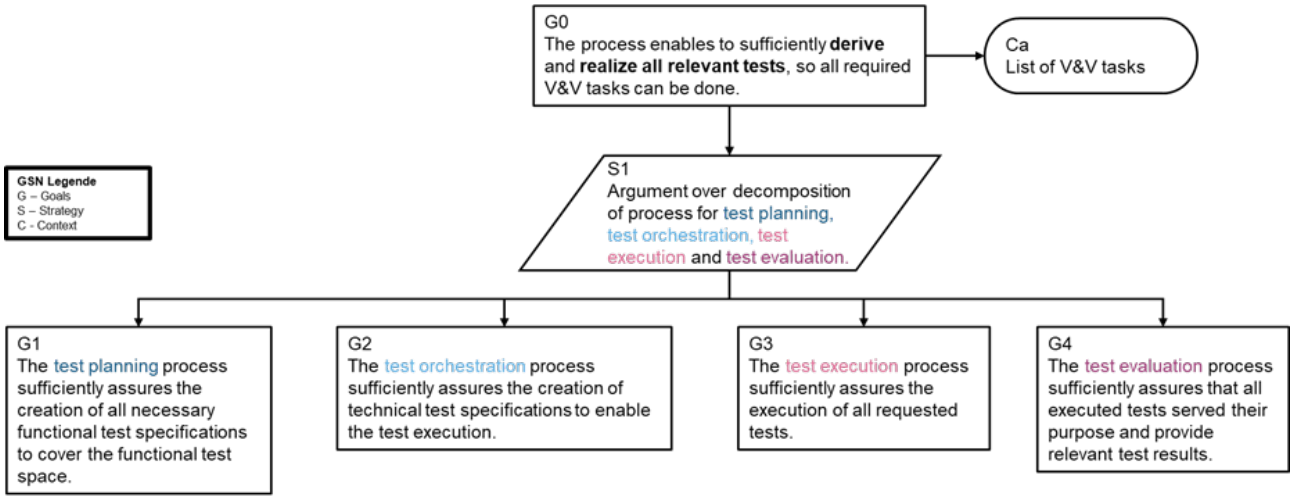


Abbildung 55: GSN für die Dekomposition der Prozessabsicherung der Testableitung und -realisierung

In Zusammenarbeit mit dem TP4/7 Ergebnis ist im Folgenden eine Detaillierung der Argumentation für die Prozesse der Testplanung und -orchestrierung entstanden. Abbildung 56 und Abbildung 57 stellen beide Argumentationsstrategien dar.

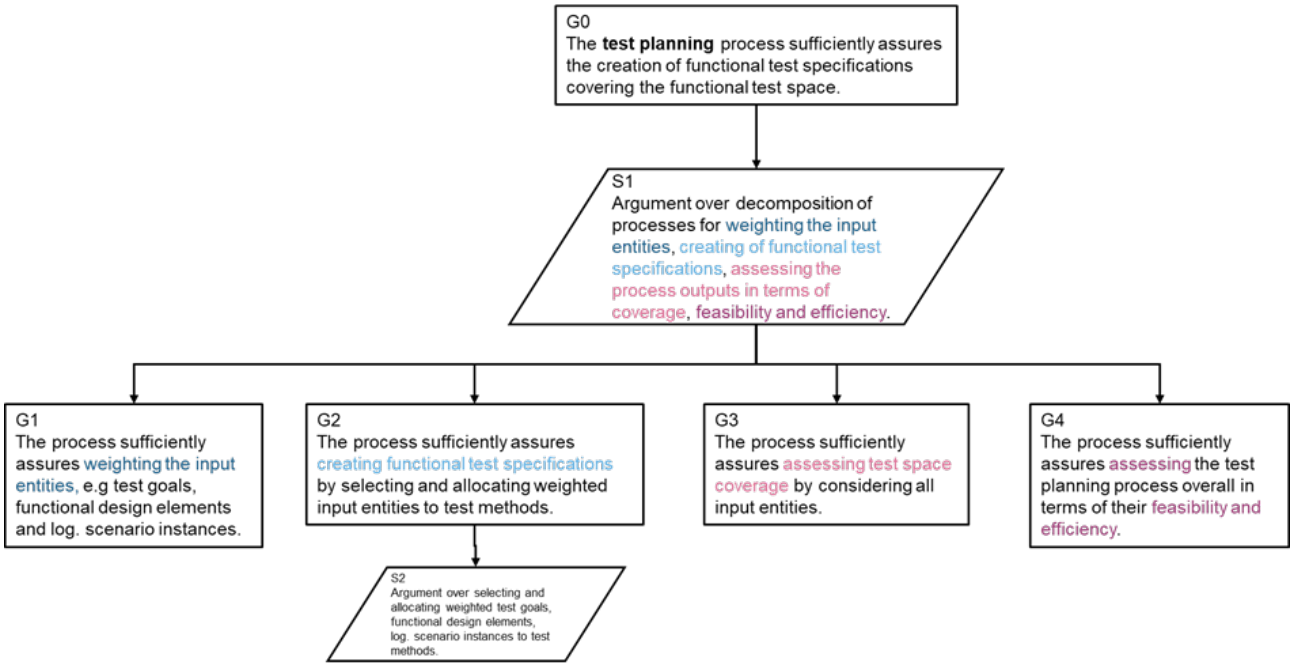


Abbildung 56: GSN für die Dekomposition der Prozessabsicherung der Testplanung

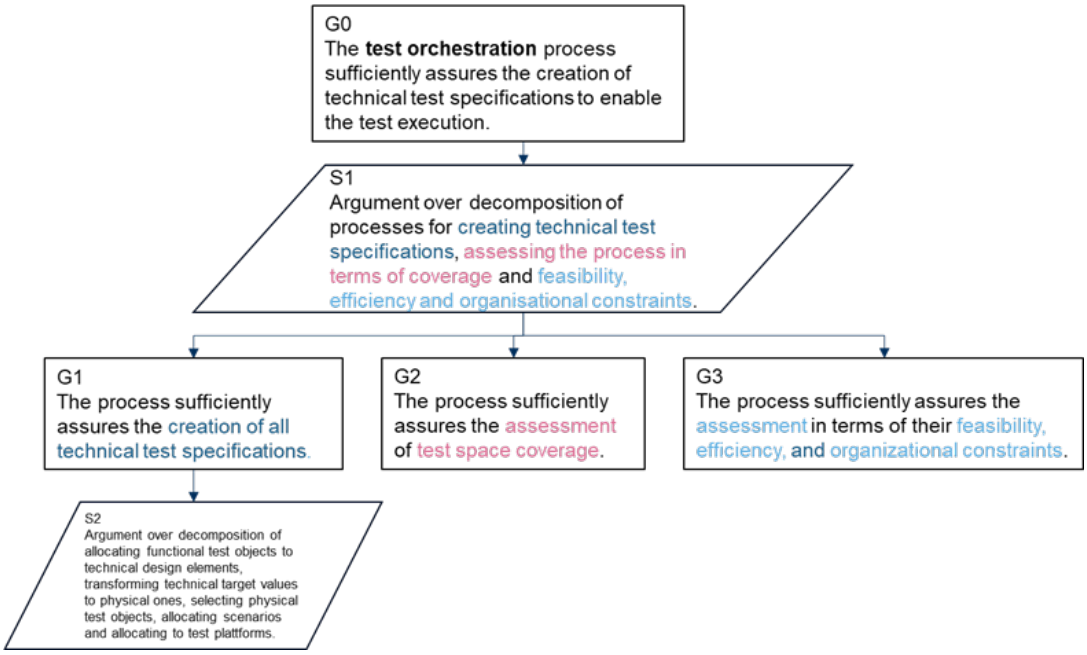


Abbildung 57: GSN für die Dekomposition der Prozessabsicherung der Testorchestrierung

Zum Überblick aller in VVM bearbeiten Prozesse zur Erstellung des V&V Systems, dient Abbildung 58 . Hier liegt der besondere Fokus auf der V&V Konzept-Erstellung (V&V Conception), welche explizit den Sicherheitsnachweis vor dem Vertrieb des ADS und während des Betriebes berücksichtigen muss.

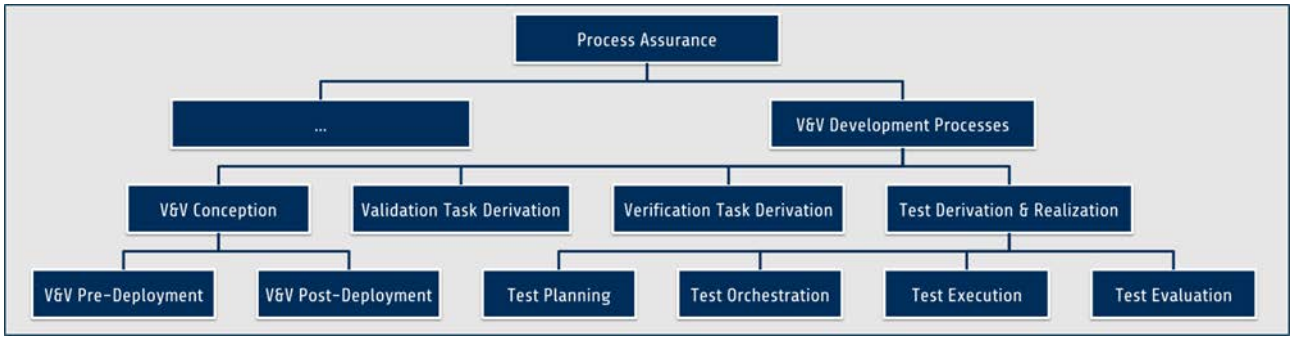


Abbildung 58: Vereinfachte Darstellung der Prozesssicherungsstruktur für die Entwicklung des V&V-Systems

Das VVM-Projekt bietet strukturierte Argumentationsmethoden für die Vorhersage von Risiken bei automatisierten Fahrsystemen (ADS) auf der Grundlage von Annahmen über relevante Entwicklungs- und V&V Artefakte. Durch diese Methoden wird es erleichtert, Entscheidungen über den Einsatz des ADS zu rechtfertigen. Außerdem bietet das Projekt einen Ausgangspunkt für weitere Argumentationsentwicklung in konkreten ADS-Projekten unter Berücksichtigung unternehmensspezifischer Absicherungsmethoden und V&V Systeme.

3.1.1.2.7 Concern Management

Neben den Argumentationsästen zur “Performance Assurance” und zur “Process Assurance” existiert in der VVM Sicherheitsargumentation ein “Concern Management”. Dieser Teil der Argumentation bezieht sich auf mögliche objektive und subjektive Zweifel relevanter Stakeholder. Damit deckt das “Concern Management” den häufig auch als “Konfidenzargument” bezeichneten Teil der Argumentation ab. Im Concern Management können sowohl Behauptungen als auch Argumentationsstrategien und Evidenz hinterfragt werden. Ziel des Concern Managements ist das Ausräumen dieser Zweifel (engl. Concerns).

3.1.1.2.8 Traceability und Durchgängigkeit

Die Entwicklung komplexer Systeme für das hochautomatisierte Fahren beinhaltet erhebliche Anforderungen an die Qualität und Zuverlässigkeit dieser Systeme. Voraussetzung für den geforderten Sicherheitsnachweis ist neben einer genauen Aufzeichnung der Konfigurationen des simulierten Systems die Sicherstellung von Rückverfolgbarkeit der zugehörigen Entwicklungsartefakte in verschiedenen Granularitäten über den gesamten Entwicklungsprozess.

Traceability-Demonstrator TRACY

Im Rahmen des VVM-Projekts wurde der Traceability-Demonstrator TRACY entwickelt, um diesen Herausforderungen zu begegnen. Die Verknüpfung einer Vielzahl konkreter Dokumente mit ihren Abhängigkeiten und zugehörigen Prozessschritten, sowie unterschiedlicher Revisionsstände, entspricht der Idee des Konfigurationsmanagements nach ISO 10007 [53]. Die VVM-Methode wurde sowohl in einem Cameo-Modell als auch in TRACY abgebildet (siehe Kapitel 3.1.2.9). Die grafische Oberfläche von TRACY ermöglicht eine einfache Navigation durch die Methodenbausteine und erhöht die Verständlichkeit durch Zuordnung der zugehörigen Entwicklungsartefakte. Zur Unterstützung der Navigation können in der Benutzeroberfläche verschiedenste Filterkriterien ausgewählt werden, mit denen z.B. der innere Aufbau der Methodenbausteine auf unterschiedlichen Detaillierungsebenen oder deren In- und Outputs für den Nutzer angezeigt werden können. In einer späteren konkreten Anwendung des Tools

ermöglicht dies dem Benutzer, den Überblick über alle Prozessschritte und Artefakte zu behalten, insbesondere wenn diese in verschiedenen Datensystemen verteilt sind. Abbildung 59 zeigt beispielhaft einen Teil der inneren Struktur der semantischen Normverhaltensanalyse.

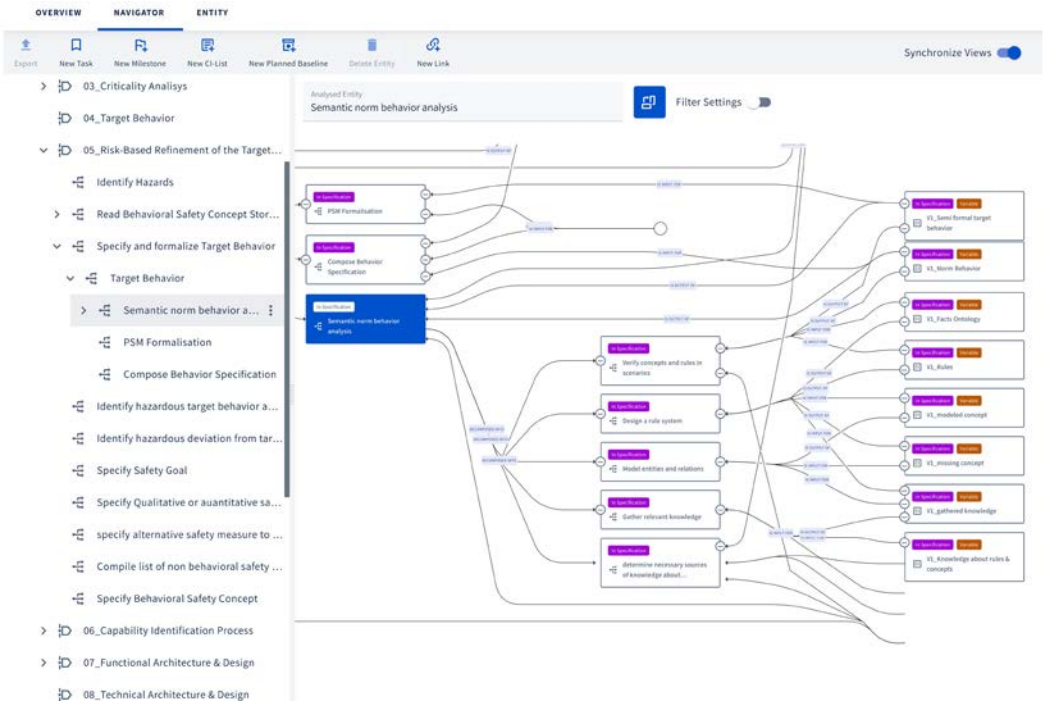


Abbildung 59: grafische Nachverfolgbarkeit zwischen Prozessen und Artefakten mit Hilfe von TRACY

VVM ODE Meta Modell Erweiterungen

Das Open Dependability Exchange (ODE) Metamodell dient als Vorlage für die Instanziierung von austauschbaren und integrierten Digital Dependability Identity (DDI) Modellen [54]. DDI-Modelle umfassen formell die Artefakte des Safety- und Security-bezogenen System-Engineerings einschließlich der Sicherheitsargumentation. Damit unterstützen sie eine formale Rückverfolgbarkeit zwischen diesen Artefakten und der Sicherheitsargumentation. Die formalisierte Natur eines DDI-Modells unterstützt die Ausführung von potentiell zeitsparenden und fehlerminimierenden automatisierten Skripten.

Im Rahmen des VVM-Projekts wurde das ODE-Metamodell erweitert, um die Rückverfolgbarkeit zwischen Artefakten von Validierungs- und Verifizierungsmethoden des Projekts zu unterstützen. Die neu eingeführten Metamodellpakete (Scenario, SOCA, Semantic Norm Behavior Analysis, Capability und PSM) beinhalten die Artefakte der Methoden zur Ableitung von Sollverhalten eines automatisierten Fahrsystems. Die Erweiterung ermöglicht eine formale Nachvollziehbarkeit zu den bereits existierenden Artefakten des ODE-Metamodells.

Automatisierte Skripte, können Entwickler folgendermaßen unterstützen:

- Wurden alle relevanten Szenarien hinsichtlich des geforderten Normverhaltens analysiert?
- Inferenz des Zielverhaltens auf Basis von PSM-Graphen-Analyse
- Herausarbeitung der berücksichtigten normativen Regeln eines bestimmten Sollverhaltes

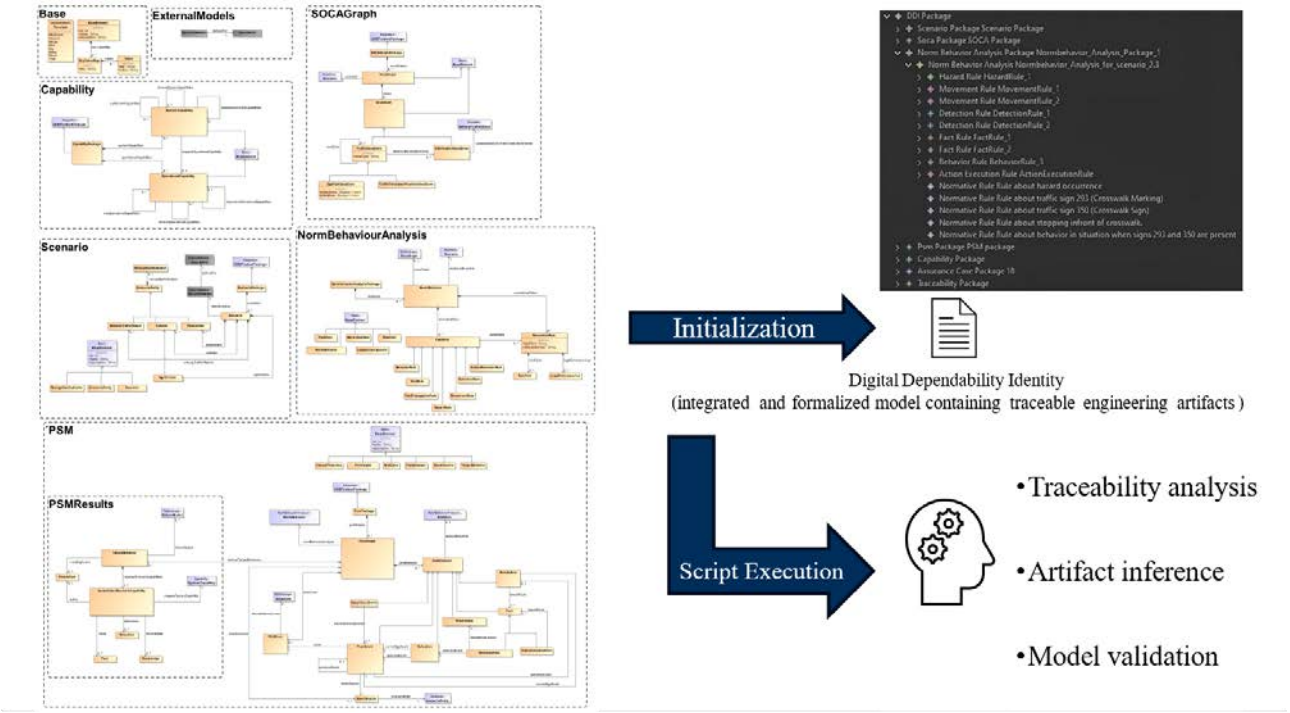


Abbildung 60: Überblick über die Verwendbarkeit der DDI

3.1.1.3 Operational Concept / ODD

Beispielhafte Kundenfunktion (KF)

3.1.1.3.1 Was ist eine Kundenfunktion?

Eine Kundenfunktion ist ein zielgerichtetes Verhalten des Produkts, das für einen realen oder abstrakten Kunden greifbar ist. Eine Kundenfunktion ist genau einem System zugeordnet. Die vollständige Beschreibung einer Kundenfunktion umfasst die folgenden Aspekte:

1. Das System, für das die KF gilt,
2. der Grund und Nutzen der KF,
3. Merkmale der KF,
4. Beziehung zur Operational Design Domain (ODD).

3.1.1.3.2 Was ist ein Automated Driving System (ADS)?

„Die Hardware und Software, die gemeinsam in der Lage sind, die gesamte dynamische Fahraufgabe (Dynamic Driving Task, DDT) dauerhaft auszuführen, unabhängig davon, ob sie auf eine bestimmte ODD beschränkt ist; dieser Begriff wird speziell zur Beschreibung eines Fahrautomatisierungssystems der Stufen 3, 4 oder 5 verwendet."

Im Rahmen der VVM-Kundenfunktion führt ein Dual-Mode-Fahrzeug einen fahrerlosen Betrieb durch, der sowohl Personen als auch Gepäck innerhalb einer definierten ODD transportiert.

„[ADS-Equipped] Dual-Mode-Fahrzeug: Ein mit ADS ausgestattetes Fahrzeug, das so konstruiert ist, dass es entweder einen fahrerlosen Betrieb unter Routine-/Normalbetriebsbedingungen

innerhalb seines gegebenen ODD (falls vorhanden) oder einen Betrieb durch einen Fahrzeugführer für vollständige Fahrten ermöglicht.” [55]

3.1.1.3.3 Operational Design Domain (ODD)

„Betriebsbedingungen, unter denen ein bestimmtes Fahrautomatisierungssystem oder ein Merkmal davon speziell für den Betrieb ausgelegt ist, einschließlich, aber nicht beschränkt auf umweltbedingte, geografische und tageszeitliche Einschränkungen und/oder das erforderliche Vorhandensein oder Nichtvorhandensein bestimmter Verkehrs- oder Fahrbahnmerkmale.” [46]

Innerhalb von VVM ist die ODD nach dem 6-Schichten-Modell strukturiert.

3.1.1.3.4 Wieso wird in VVM eine Kundenfunktion benötigt?

Der KF wird benötigt, um eine grundlegende funktionale Beschreibung des Verhaltens des ADS in einer bestimmten ODD zu erhalten. Unter Berücksichtigung dieser Voraussetzung kann das Verhalten des ADS für die spezifischen Functional Use Cases (FUC) innerhalb von VVM abgeleitet werden.

Merkmale

- Steuerung der Längs- und Querbewegung des Fahrzeugs bis zu 60 km/h in städtischen Umgebungen sowie 100 km/h auf Autobahnen mit oder ohne Zielfahrzeug
- Planung von Trajektorien
- Einhaltung der relevanten Verkehrsregeln
- Beherrschen von vorgegebenen Kurvenradien und Fahrbahnbreiten
- Fahren auf und von Autobahnen
- Wechsel der Fahrbahn durch Kreuzungen
- Parkmanöver
- Anfahren aus dem Stillstand und Herausfahren in den Verkehr
- Reaktionen des Navigationssystems auf Stauwarnungen, Straßensperrungen und Baustellen
- Fahren bei Nacht mit künstlicher Straßenbeleuchtung
- Umgang mit typischen Wetterbedingungen
- Abbiegen unter Berücksichtigung des Gegenverkehrs
- Fahrspurwechsel auf mehrspurigen Straßen (z. B. Bushaltestelle, Radfahrer, parkende Autos)
- Vorbeifahren an Ampeln
- Befolgen von Fußgängerüberwegen
- Durchführen von Manövern mit minimalem Risiko

- Anpassen an den Verkehrsfluss

Aus Gründen der Vereinfachung werden folgende Situationen nicht von der beispielhaften Kundenfunktion abgedeckt

- Spielstraßen
- Straßen mit Gegenverkehr und ohne Mittellinie
- Kreisverkehre
- Anweisungen von Polizeibeamten und Einsatzfahrzeugen

3.1.1.3.5 Gesetzeslage/ State of the Art: EU Level 4, AFGBV

AFGBV

Die Änderung des Straßenverkehrsgesetzes (StVG) im Juli 2021 und die damit verbundene Automatisiertes Fahren Genehmigungs- und Betriebsverordnung (AFGBV) stellt einen bedeutenden Schritt in Richtung automatisierter und autonomer Fahrfunktionen im öffentlichen Straßenverkehr dar. Durch diese Änderung wird das Tor geöffnet für die nationale Typgenehmigung von Fahrzeugen, die mit automatisierten oder autonomen Fahrfunktionen ausgestattet sind. Dies ermöglicht die rechtliche Anerkennung und Regulierung dieser modernen Fahrzeugtechnologien.

Des Weiteren werden automatisierte Testfahrzeuge zugelassen. Dies eröffnet Möglichkeiten für gezielte Tests und Entwicklungsaktivitäten unter kontrollierten Bedingungen, um die Leistungsfähigkeit und Sicherheit dieser Fahrzeuge zu verbessern.

Besonderheit der AFGBV ist, dass es keine Begrenzung auf bestimmte Fahrzeugklassen gibt. Damit werden automatisierte und autonome Fahrfunktionen nicht mehr ausschließlich auf bestimmte Fahrzeugtypen beschränkt.

Insgesamt schafft diese Änderung des StVG einen rechtlichen Rahmen, der die Entwicklung und Integration von automatisierten und autonomen Fahrfunktionen in Deutschland vorantreibt und den Weg für innovative Lösungen im Bereich des Straßenverkehrs ebnen soll.

Besonderheit ist, dass neben der Fahrzeuggenehmigung durch den Hersteller autonome Fahrzeuge in Betriebsbereichen eingesetzt werden dürfen, die vorab durch den Halter genehmigt werden müssen.

EU-Level 4

Die im Juli 2022 erschienene Verordnung auf EU-Ebene, anwendbar für Fahrzeuge der Klassen M und N gemäß Verordnung (EU) 2018/858, stellt einen wichtigen Schritt in der Entwicklung automatisierter Fahrzeugtechnologien auf EU-Ebene dar. Diese Regelung sieht vor, dass die Implementierung automatisierter Fahrfunktionen zunächst auf Fahrzeuge der Klassen M (Personenkraftwagen) und N (Nutzfahrzeuge) beschränkt ist.

Des Weiteren ist die Anwendung dieser Regelung auf Kleinserien begrenzt. Dies bedeutet, dass die Produktion automatisierter Fahrzeuge zunächst in begrenztem Umfang erfolgt, was es den Herstellern ermöglicht, die Technologie schrittweise zu entwickeln und zu verbessern, bevor sie in großem Maßstab eingesetzt wird.

Darüber hinaus ist die Nutzung automatisierter Fahrfunktionen gemäß dieser Regelung auf bestimmte Use-Cases begrenzt, darunter Personentransport, Hub-to-Hub-Verkehr und Automatisiertes Valet-Parking (AVP).

Insgesamt trägt diese Regelung dazu bei, die Einführung automatisierter Fahrzeugtechnologien EU-weit zu regulieren. Sie legt einen Rahmen fest, der die Sicherheit und Effizienz dieser Technologien gewährleistet und gleichzeitig Innovationen fördert. Der Einsatz der Fahrzeuge ist jedoch national geregelt. Das bedeutet, dass jedes EU-Land den Betrieb selbstständig regeln kann. In Deutschland beispielsweise erfolgt die Regelung über die AFGBV. Das bedeutet, dass das Fahrzeug zwar nach der EU-Verordnung genehmigt werden kann, der Betrieb jedoch nach AFGBV erfolgt. D.h. ein Betriebsbereich muss durch den Halter genehmigt werden.

Abbildung 61: Rechtliche Stakeholder bei der Zulassung automatisierter und autonomer Fahrzeuge

3.1.1.3.6 Regelkonformes Verhalten im Straßenverkehr

In Deutschland regelt die StVO [56] das Zusammenleben im Straßenverkehr. Ziel und Leitbild der StVO ist es, einen sicheren und rücksichtsvollen Umgang im Straßenverkehr zu schaffen, der sich insbesondere aus §1 StVO ergibt. Die StVO richtet sich an alle Verkehrsteilnehmer, also auch an ein ADS.

ADS muss ein regelkonformes Traffic-Verhalten aufweisen

Der Betrieb von AD-Systemen im Straßenverkehr erfordert die Bestätigung der Einhaltung der Verhaltensanforderungen in Bezug auf Kollisionsfreiheit, ein für andere Verkehrsteilnehmer verständliches Verhalten und die Erfüllung der geltenden Verkehrsregeln im Einsatzgebiet. Die Einhaltung von Verkehrsregeln (StVO) und die Vermeidung von Verkehrsverstößen (Bußgeldkatalog) sind zentrale Anforderungen an das Zielverhalten.

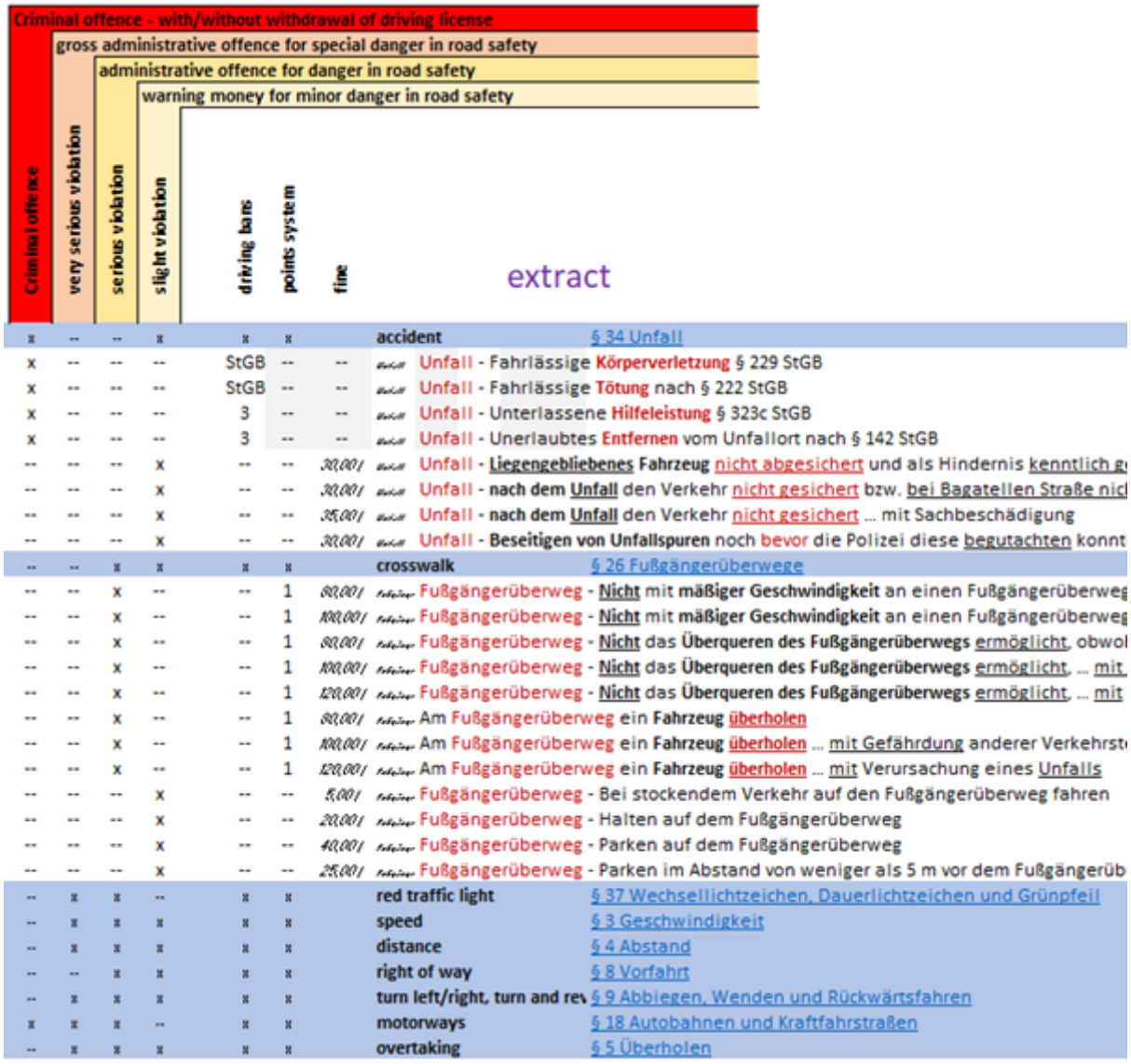


Abbildung 62: Gewichte für gefährliche Ereignisse gemäß Bußgeldkatalog

Quantifizierte Kriterien für das Verkehrsverhalten

Grundvoraussetzung für die Zulassung zum Straßenverkehr ist eine quantifizierte Spezifikation der Verhaltensbeschreibungen mittels konkreter Qualitäts- und Toleranzkriterien. Es muss eindeutig angegeben und nachprüfbar sein, welches Verkehrsverhalten "noch legal" und welches "nicht mehr legal" ist.

Durch einen methodischen Ansatz in 5 Schritten können Quellen verwendet werden, um notwendige, quantifizierte Spezifikationswerte zu ermitteln (siehe auch Abbildung 63):

1. Ermittlung der relevanten Quellen des Verkehrsverhaltens im Zielland.
2. Ableitung der für die Szenario-Beschreibung relevanten Zielvorgaben des konformen Verkehrsverhaltens.
3. Direkte Quantifizierung der Verkehrsverhaltensanforderungen anhand der zulässigen Grenzwerte aus den Gesetzestexten der Verkehrsregeln.

4. Konkretisierung der Quantifizierung des noch offenen Handlungsspielraums anhand des relevanten Verkehrsverhaltens auf Basis verkehrsrechtlicher Urteile.

5. Entwicklung, Argumentation, Evidenz und rechtlicher Vergleich der entwickelten Grenzwerte der jeweiligen Verkehrsverhaltensspezifikation.

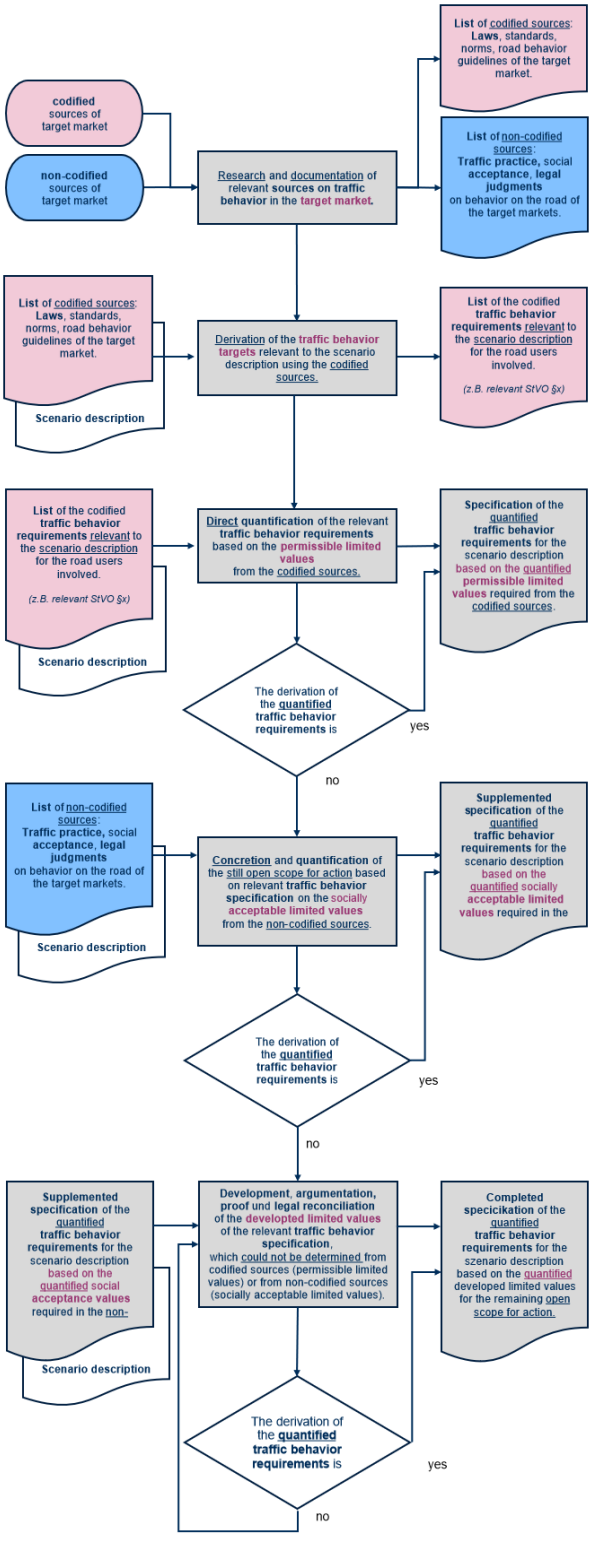


Abbildung 63: Schritte zur Bestimmung des quantifizierten Verkehrsverhaltens

3.1.1.3.7 Operational Design Domain (ODD)

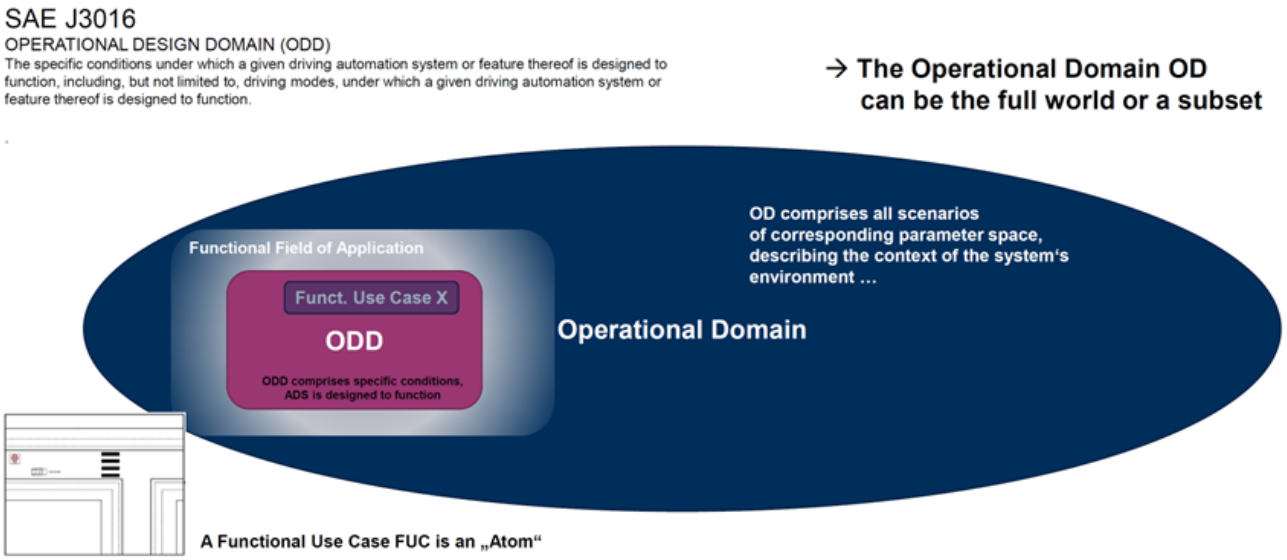


Abbildung 64: Zusammenhang zwischen OD, funktionalem Anwendungsbereich und ODD (© VVM)

Gemäß ISO:34503 „“An ODD defines the operating conditions under which an ADS is designed to operate safely.“ Dieser Standard baut auf den ODD-Begriff von SAE J3016, führt zusätzlich die Begriffe Target Operational Domain und Current Operational Domain (TOD, COD) ein und definiert einen Vorschlag für Attributstruktur (Taxonomie).

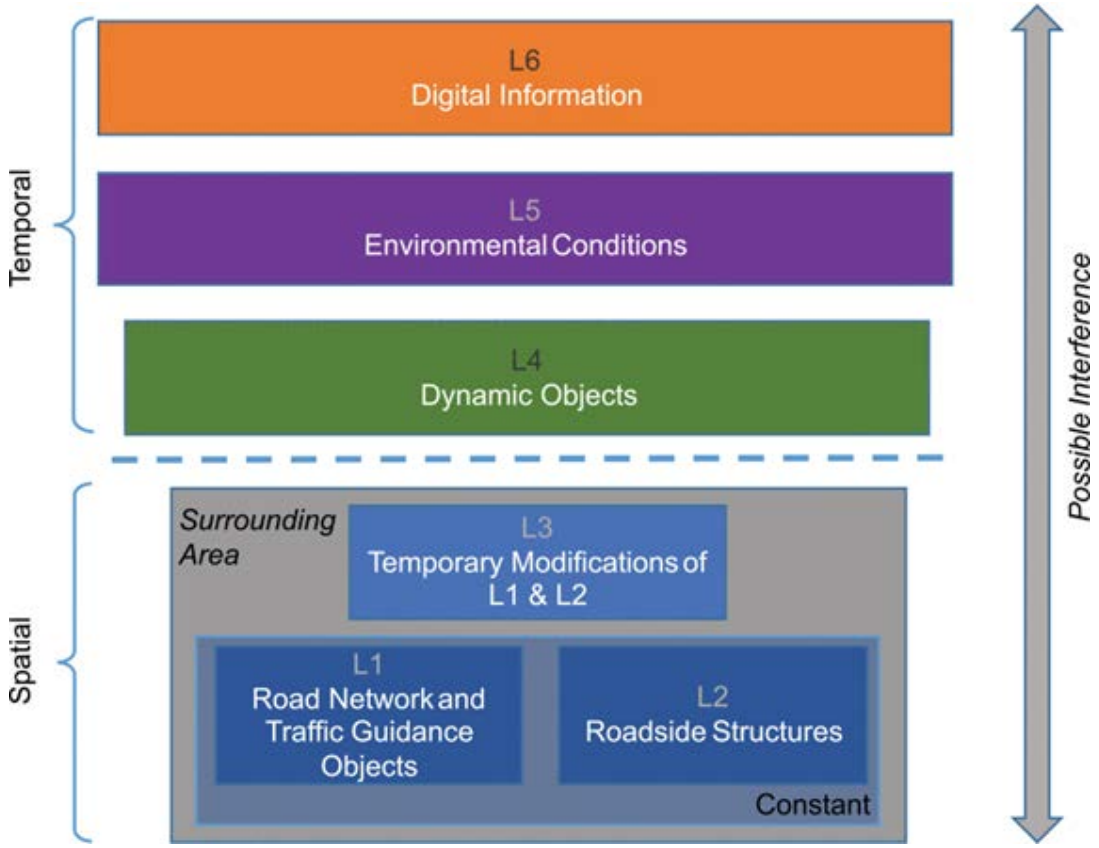


Abbildung 65 Abbildung 2: 6-Layer Model (6LM) als Operational-Domain-Beschreibungssprache [46] (© VVM)

VVM Ergebnisse

- Die Sprache zur Beschreibung und Analyse der Operational Domain (OD) in VVM ist das 6-Layer-Modell (6LM) aus dem PEGASUS-Projekt. Diese Beschreibungssprache wurde detailliert und verbessert [46]. Eine umfassende Implementierung dafür ist die A.U.T.O-Ontologie, diese wird für Kritikalitätsanalyse verwendet [57].
- Für die OD-Analyse und die Verfeinerung des funktionalen Anwendungsfalls (VVM FUC 2.3) ist die 6LM-Erweiterung angewendet worden. Als Ergebnis sind Szenarien [57] [58] entstanden. Diese Kernszenarien umfassen angemessen abstrakt für die designierte Kundenfunktion (KF) die angestrebte ODD.
- Die abgeleiteten logischen Szenarien definieren die Zusammensetzung der ODD und bestimmen dadurch den Testraum.
- Methode für Definition der Einflussparameter und entsprechende Stichprobenstrategie für Abdeckung des Testraums durch konkrete Szenarien ist als [45] veröffentlicht.

→ Die ODD in VVM wird als Zusammensetzung der parametrisierten während der Produktentwicklung erstellten Szenarien aufgefasst.

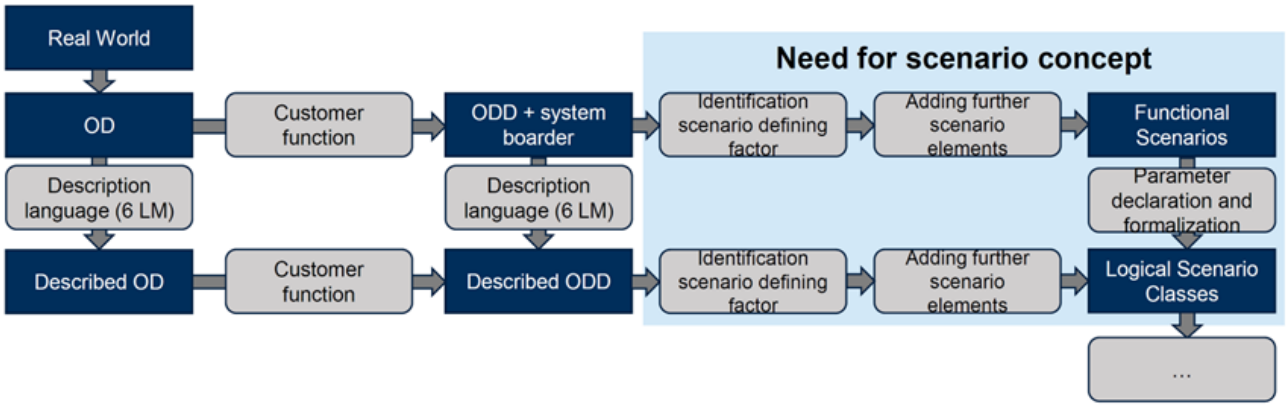


Abbildung 66: Workflow Realitätsabstraktion (© VVM)

- Der funktionale Anwendungsbereich entspricht in etwa dem Begriff ISO:34503 **TOD**
- Das Omega-Format [59] bietet die Möglichkeit, die Fahrten/Simulationsergebnisse als Schnappschüsse der Verkehrsumgebung (vergleichbar mit **COD** in ISO:34503) als konsistenten Daten zu sammeln. Das Omega-Format (und die dazugehörige Python-Bibliothek) ist eine weitere Implementierung des 6LM-Konzepts.

Iterative Verfeinerung von ODD und Kundenfunktion

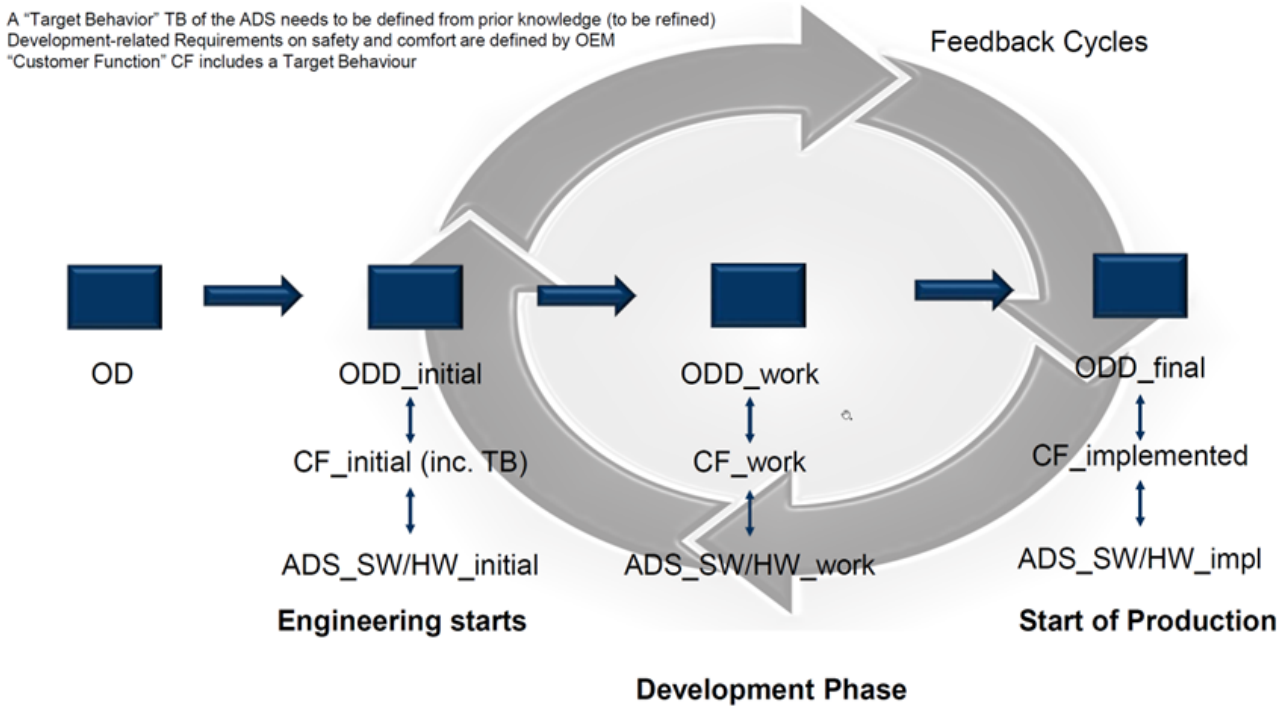


Abbildung 67: Feedbackschleifen und iteratives Konzept für die ODD-Entwicklung (© VVM)

Verbleibende offene Fragen

- Eine Explizierung der ODD-Beschreibung als separates Artefakt bleibt eine offene Aufgabe für die Zukunft. Ein ODD-Beschreibungsformat wird derzeit im ASAM OpenODD-Projekt entwickelt. Eine kompakte, menschen- und maschinenlesbare Darstellung bleibt weiterhin eine Herausforderung, mehrere laufende Aktivitäten adressieren dies.

- Eine weitere offene Frage ist, wie das zu erwartende Verhalten dynamischer Objekte (z.B. Straßennutzungskultur, Charakter der Verkehrsteilnehmer von aggressiv bis kooperativ) außerhalb des Szenarios als ODD-Parameter modelliert werden kann.

3.1.1.3.8 Top Goals

„Top Goals“ beschreiben notwendige Aktivitäten für die Realisierung von Erwartungen an eine Methode und deren Verwendung zum Testen eines "automatisiertes Fahrsystem" (ADS).

Abbildung 68: Beispielhafte Stakeholder Anforderungen in Kombination mit möglichen Concerns als möglichen Input für die Ableitung von Top-Zielen © Robert Bosch GmbH

Wir haben eine Systematik entwickelt, um "Top Goals" wie folgt abzuleiten:

- Erwartungen werden in Form von Fähigkeiten abstrahiert
- Fähigkeiten werden dekomponiert, bis diese durch die Erwartungen vollständig abgedeckt sind
- aus den Dekompositionen werden Top-Goals extrahiert

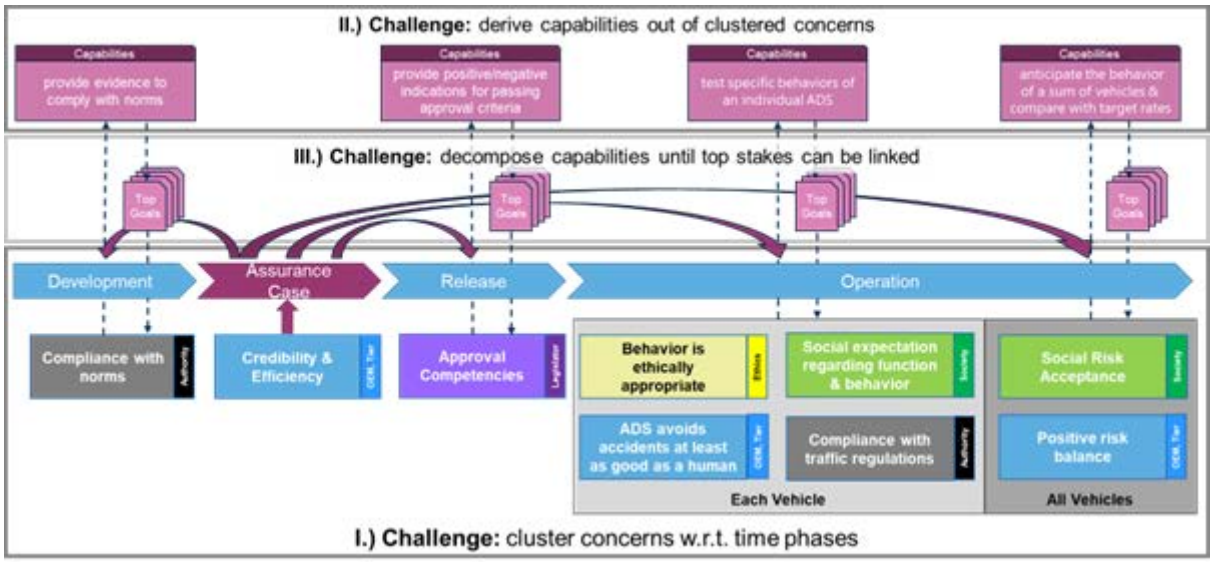


Abbildung 69: Herausforderungen bei der Ableitung von Top-Zielen. Zunächst ordnen wir Concerns der entsprechenden Zeitphase zu. Zum Beispiel müssen wir während der Freigabe des Produkts Genehmigungskompetenzen nachweisen, was zur Zeitphase „Release“ gehört, obwohl diese Fähigkeiten bereits im Rahmen des Assurance Cases vorhanden sein müssen. Nachfolgend werden Concerns aggregiert und in Form von Fähigkeiten abstrahiert. Abschließend werden diese

abstrahierten Fähigkeiten so lange dekomponiert, bis alle Concerns der Stakeholder vollständig abgedeckt und somit operationalisiert werden können (© Robert Bosch GmbH).

3.1.1.3.9 Das Verfahren

Abbildung 69 zeigt das entwickelte Verfahren zur Ableitung von Top Goals. Als erstes werden die Concerns der Stakeholder in den jeweiligen Zeitphasen geclustert. Nachfolgend werden notwendige Fähigkeiten zur Realisierung der geclusterten Concerns definiert. Es wird darauf hingewiesen, dass durch das Zusammenfassen (clustern) eine Menge von Concerns nun durch eine einzige Fähigkeit dargestellt werden kann. Schließlich wird jede Fähigkeit so lange dekomponiert, bis alle Aspekte der jeweiligen Concerns berücksichtigt sind, so dass die Realisierung dieser Fähigkeiten zur Umsetzung der Concerns führt.

3.1.1.3.10 Dekomposition der Fähigkeiten

In Abbildung 70 wird gezeigt wie Concerns auf Redundanz und Widerspruchsfreiheit unter Verwendung von Hierarchisierungsebenen geprüft werden, so dass Mehraufwände infolge von Duplikaten oder in Konflikt stehenden Concerns vermieden werden können. Zur Auflösung von Konflikten sind zusätzliche Fähigkeiten zu formulieren, so dass eineindeutig hervorgeht welcher Concern in welcher Situation umzusetzen ist.

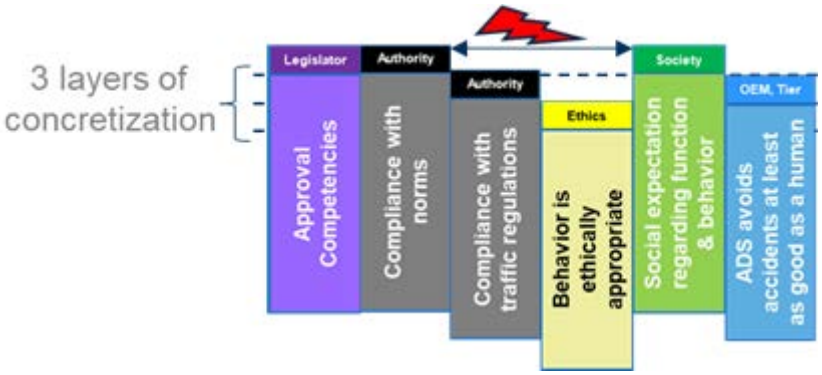


Abbildung 70: Unterschiedliche Hierarchieebenen von Concerns sowie ein Konflikt (als roter Blitz dargestellt) zwischen "Einhaltung von Normen" & "sozialer Erwartung in Bezug auf Funktion & Verhalten". Zwischen beiden Concerns können Konflikte auftreten, da beispielweise menschliche Fahrer von Zeit zu Zeit Stoppschilder überfahren, was zum Teil erwartet wird aber nicht den Normen entspricht (© Robert Bosch GmbH).

3.1.1.4 Szenarienabstraktion Grundlagen (Realitätsabstraktion)

Szenarien sind zentraler Bestandteil des Testkonzepts von VVM. Im Rahmen der VVM-Gesamtmethode werden durchgängig Szenarien als Modell für den Entwicklungsraum sowie den Absicherungs- bzw. Testraum benutzt (siehe Abbildung 71). Mit der kontinuierlichen Validierung des Szenariomodells ist dies ein Beitrag zum Schließen der Spezifizierungslücke. Die Grundlagen dazu werden in diesem Abschnitt dargelegt.

3.1.1.4.1 Die Rolle der "Realitätsabstraktion" in der szenariobasierten Entwicklung eines ADS

Unter dem Begriff der *Realitätsabstraktion* wird eine Methode verstanden, ein hinreichend vollständiges szenariobasiertes Modell der ODD zu erstellen. Das Ergebnis ist eine Menge von CORE-Szenarien (funktional oder logisch) und eine Szenario- (Parameter) - Datenbank. Diese ermöglichen es, die ODD (hier: Verkehr und Umgebungsbedingungen in der Ziel ODD der Kundenfunktion zu formalisieren bzw. zu modellieren. Das Ergebnis der Realitätsabstraktion -die

drei Elemente Menge CORE Szenarien (funktional und logisch) und Szenario (Parameter) Datenbank werden als ODD-Metamodell bezeichnet. (siehe Abbildung 71)

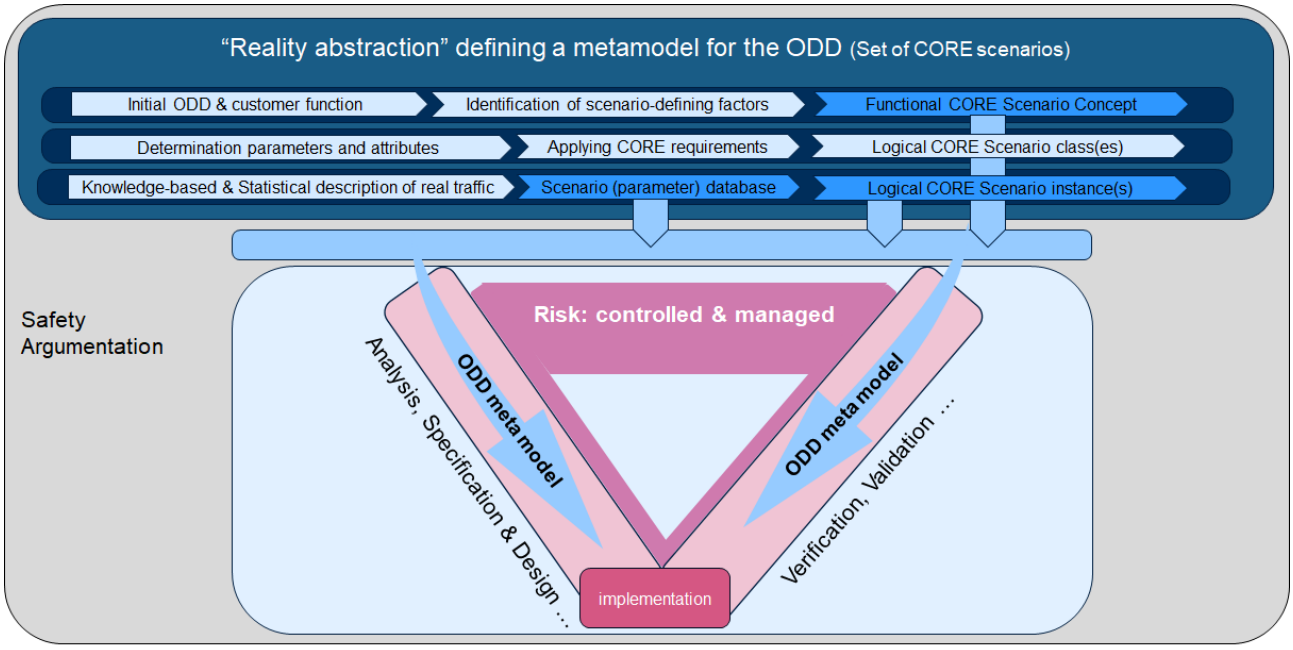


Abbildung 71: Realitätsabstraktion im Kontext der VVM-Gesamtmethode

Ausgangsbasis ist das 6-Ebenen-Modell, das in PEGASUS für den Anwendungsfall Autobahn entwickelt wurde. Die Anwendung des Modells auf eine urbane ODD erfordert Anpassungen in den Ebenen 1 und 4. Es wurde ein neues Konzept zur Beschreibung der Grundkonstellationen oder Basisszenarien für die dynamischen Objekte der Ebene 4 entwickelt, die sich sowohl für das Einsatzgebiet Autobahn - Straßen mit mehrspurigen und getrennte Richtungsfahrbahnen - als auch auf urbane Domänen verwenden lassen. Dieser Ansatz wird durch ein Konzept von ganzheitlichen städtischen Fahrszenarien ergänzt, die je nach dem Grad der Interaktion mit anderen Instanzen kategorisiert werden. Die neuen Szenariotypen kombinieren Strukturelemente der Ebene 1 mit Interaktionsmustern der Ebene 4. Das Konzept wird später in diesem Kapitel im Detail vorgestellt. (siehe 3.1.1.4.2)

Der Begriff Szenario hat unterschiedliche Inhalte und Darstellungsweisen im Entwicklungsprozess, weil unterschiedliche Entwicklungsphasen aufgrund ihrer abzuarbeitenden Entwicklungsschritte unterschiedliche Anforderungen an die Nutzung von Szenarien haben (siehe Abbildung 27). Die Konzeptphase beschreibt Szenarien auf einem hohen Abstraktionslevel. Die Systementwicklung und insbesondere die Testspezifikation im Rahmen der Validierung und Verifikation benötigen zur Strukturierung des Testens in der Testplanung eine Beschreibung der Szenarien in Parameterbereichen des physikalischen Zustandsraums. Das eigentliche Testen also die Ausführung und Bewertung eines Testfalls benötigt eindeutig definierte, zu testende Szenarien. Um diesem Anspruch gerecht zu werden, werden Szenarien auf drei Abstraktionsebenen definiert: funktional, logisch und konkret.

Funktionales Szenario: Ein funktionales Szenario stellt eine verhaltensbasierte Beschreibung eines Szenarios auf einer semantischen Ebene dar. Die Entitäten und deren Beziehungen untereinander werden formuliert. Die Formulierung ist widerspruchsfrei. Die Beschreibung kann verbal (natürlichsprachlich) oder mit einer formalen Sprache, visuell (grafisch) oder auf anderer Art erfolgen.

> *Ein funktionales Szenario beschreibt relevante Akteure und ihre betrachteten Grundmanöver. Es handelt sich um eine (bewusst) unspezifische Beschreibung eines Szenarios in natürlicher Sprache, die nicht nur konkrete Parameter oder deren Spektren, sondern auch einige grundlegende Informationen offen lässt.* (Definition aus PEGASUS)

Logisches Szenario: Ein logisches Szenario stellt eine formalisierte Beschreibung eines Szenarios dar. Es hat deklarierte Attribute und Parameter für das korrespondierende funktionale Szenario. Es nutzt dazu insbesondere die Beschreibungssystematik des 6-Ebenen-Modells. Es kann unbeschränkte Parameterräume aber auch beschränkte Parameterbereiche oder bei diskreten Parametern deren Enummerationen sowie die Abhängigkeiten von Parametern enthalten.

> *Ein Logisches Szenario beschreibt relevante Akteure und ihre betrachteten Grundmanöver formal. Entitäten und Beziehungen unter diesen werden parametrisch formuliert. Bereiche für die Parameter und. Beziehungen zwischen Parameterbereichen können angegeben sein.* (Definition aus PEGASUS)

Für ein logisches Szenario kann es zwei besondere Ausprägungen geben:

1. Alle Parameter sind festgelegt, ihnen wurde (noch) kein Parameterbereich zugewiesen.
2. Alle Parameter sind festgelegt, jedem wurde ein Parameterbereich zugewiesen.

Um dies sprachlich fassen zu können wurden neue Begriffe eingeführt:

Die logische **Szenarioklasse** ist ein logisches Szenario, für das die beschreibenden Parameter festgelegt wurden.

Die logische **Szenarioinstanz** ist eine Szenarioklasse, bei der jedem Parameter ein (gültiger) Wertebereich zugeordnet wurde.

Konkretes Szenario: Ein konkretes Szenario entsteht durch die Instanziierung einer logischen Szenario-Instanz, indem diese mit konkreten Werten gefüllt wird.

> *Ein konkretes Szenario weist allen Parametern eines logischen Szenarios konkrete Werte zu. Es modelliert eine diskrete Zuordnung/Auswahl von Parametern über möglicherweise kontinuierliche Spektren eines logischen Szenarios.*
>
> *Ein konkretes Szenario stellt ein parametriertes Modell mit festen Parametern der zeitlichen Abfolge von Szenen (logisches Szenario) dar, welches mit einer konkreten Startszene beginnt. Alle Parameter, die ein Verkehrsereignis beschreiben, sind im konkreten Szenario explizit festgelegt. Zu einem Zeitpunkt findet genau ein konkretes Szenario statt*. (Definition aus PEGASUS)

Die Abstraktionslevel insbesondere die Ebenen funktional, logisch und konkret sind an die unterschiedlichen Anforderungen an Prozessschritte im Entwicklungsprozess angepasst (siehe Abbildung 74). Sie dienen den Entwicklern dazu, ein Modell der ODD durchgängig nutzen zu können und den fortschreitenden Erkenntnisgewinn in dem gleichen Modell integrieren zu können. Diesem Zweck dienen die verbalen bzw. grafischen Beschreibungsformen. Ein anderer Adressat sind die in dem Prozess eingesetzten Tools. Hier finden formale Sprachen Anwendung- insbesondere die in PEGASUS vorgeschlagenen Sprachen OpenSCENARIO und OpenDRIVE - die eine Kopplung zur Simulations und deren Entwicklungs- und Testplattformen ermöglichen.

Für die Verwendung von Ontologien, wie insbesondere der AUTO Ontologie (siehe Kapitel 3.1.1.4.6), ist eine besondere Art der formalisierten Beschreibung wichtig. Dies führt zu der Definition eines abstrakten Szenarios.

Abstraktes Szenario: Ein abstraktes Szenario ist eine formalisierte, deklarative Beschreibung eines Szenarios mit dem Fokus komplexe Zusammenhänge, insbesondere Wirkzusammenhänge, darzustellen. Die Semantik der Beschreibung orientiert sich hierbei an der verendeten Ontologie.

Ein abstraktes Szenario ist maschinenlesbar und generiert eine Szenariobeschreibungssprache wie zum Beispiel OpenSCENARIO und OPENDRIVE (siehe Settings aus PEGASUS).

Abstraktionslevel definieren den Detaillierungsgrad in der Beschreibung eines Szenarios. In der Anwendung dieser Konstrukte ist aber auch die “Grammatik” und der “Wortschatz”, welche zur Beschreibung der Entitäten, deren Beziehungen und Grundverhalten eines Szenarios verwendet werden, von Bedeutung. VVM verwendet hier insbesondere das mit PEGASUS etablierte, systematische 6-Ebenenmodell (siehe Abbildung 72).

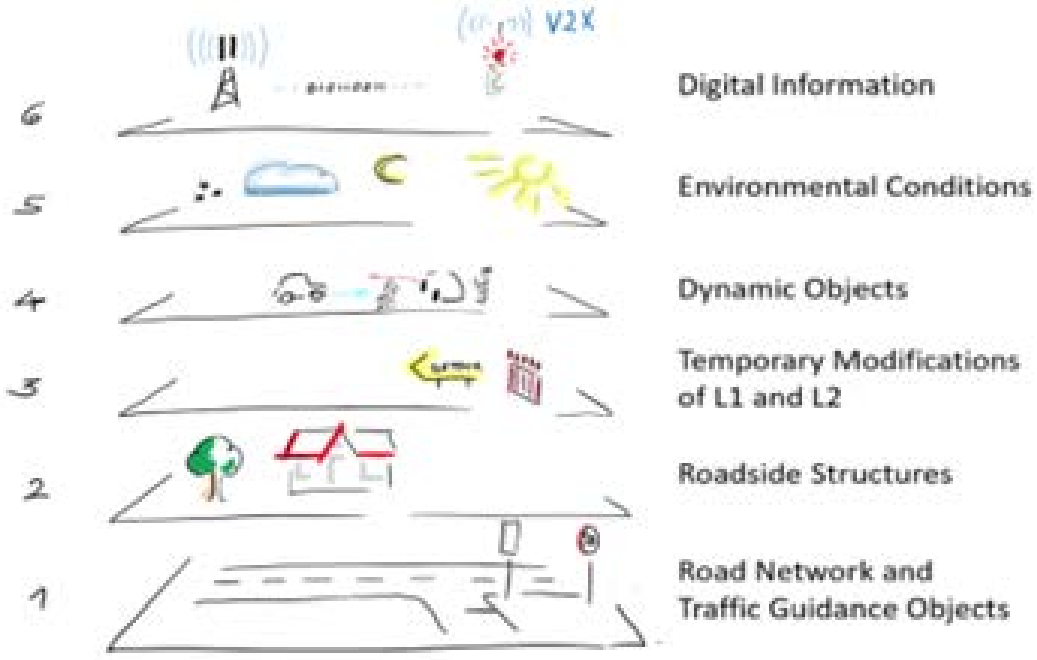


Abbildung 72: 6-Ebenen-Modell [46] zur Beschreibung eines Szenarios.

Das Modell wurde für eine Anwendung auf Autobahnen und urbanen Gebieten erweitert. Details werden in Kapitel 3.1.1.4.2 dargestellt.

Neben Abstraktionslevel (funktional, logisch, konkret) und Beschreibungssystematik (6-Ebenen-Modell) ist für die VVM-Gesamtmethode ein weiterer Begriff von zentraler Bedeutung: die Menge der CORE-Szenarien. Bildlich spannen sie den Szenarienraum auf bzw. überdecken sie den Szenarienraum hinreichend vollständig. Die Analogie aus der Mathematik sind die Menge der EINHEITSVEKTOREN in der linearen Algebra, die den Vektorraum (z.B. R^n) aufspannen oder in der Maßtheorie die Borellmengen, die komplexe Gebilde überdecken und so messbar machen.

Für ein Modell der ODD benötigen wir - neben Abstraktionslevel und Beschreibungssystematik - eine (kleine) Menge von (Äquivalenzklassen von) Szenarien die in Gänze die Menge aller Szenarien in der ODD hinreichend vollständig repräsentieren. Wie dieser Nachweis für die Trias

Abstraktionslevel, Beschreibungssystematik, Menge der CORE-Szenarien zu führen ist, findet sich in Kapitel 3.1.1.4.5.2.

Die Menge der CORE-Szenarien ist definiert als eine Menge repräsentativer Klassen funktionaler/logischer Szenarien. Sie sind bestimmt als

- die kleinste Menge von logischen/funktionalen Szenarien, die die bekannten Typen von Nutzungsfällen beschreiben, die in der ODD für die Kundenfunktion im Rahmen einer sicheren und konformen Verhaltensweise der Kundenfunktion innerhalb einer sicheren und konformen ODD auftreten können;
- deren zugrundeliegende Basisszenarien disjunkt sind. Diese Szenarien definieren dynamische Basisbewegungskonstellationen;
- die die ODD hinreichend vollständig repräsentieren;
- für deren Klassen die kleinste Menge von Parametern deklariert wurde, die in jedem Element der Menge der logischen Szenarien die bekannten Kategorien von Parametern repräsentieren, die für die Kundenfunktion in der ODD im Rahmen der logischen Szenarien relevant sind;
- die nach Relevanz/Exposition in der ODD geordnet sind.

Das in VVM verwendete ODD Metamodell umfasst eine Menge von funktionalen sowie logischen CORE Szenarien (Klassen / Instanzen) sowie die Szenario-Datenbank.

Das Metamodell für ODD erfüllt die Anforderung nach Dekomposition des Szenarienraums in Bezug auf seine Verwendung als Testraum im Rahmen der Verifikation und Validierung:

- Das Metamodell ist in CORE-Szenarien zerlegbar,
- jedes CORE-Szenarios ist in Beschreibungsebenen zerlegbar,
- jede Beschreibungsebene ist in Kategorien zerlegbar,
- jede Kategorie ist in Parameter zerlegbar.

Im Rahmen des Entwicklungsprozesses werden valide Bereiche für die Szenario-Parameter definiert (Szenario-Instanz).

Die Idee der CORE-Szenarien ist es, ein Modell der ODD zu erstellen. Dabei werden Basisszenarien verwendet, um die ODD so vollständig wie möglich darzustellen. Somit kann man dieses Modell durchgängig als Repräsentant der Betriebssituationen und Zustände der ODD verwenden. Abbildung 73 veranschaulicht dies. Es kann gezeigt werden, dass die CORE-Szenarien ein hinreichend vollständiges Modell der ODD darstellen [46] (Siehe auch Kapitel 3.1.1.4.5.2).

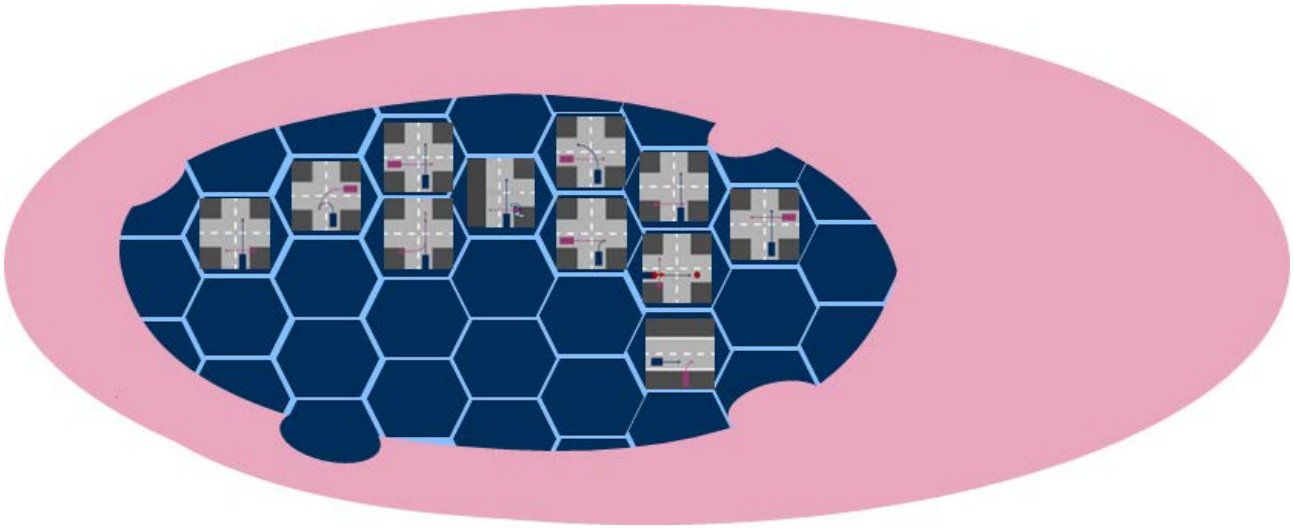


Abbildung 73: OD (rosa) und ODD (dunkelblau) überdeckt mit CORE-Szenarien (Waben)

Die CORE Szenarien können formalisiert als Ontologie beschrieben werden. VVM nutzt die formalisierte Darstellung des Szenario-Modells und verknüpft sie mit “Wissen” über die Betriebsdomäne. Dies bildet die Basis für die A.U.T.O. Ontologie (siehe auch Kapitel 3.1.1.4.6). Eine Ontologie im Sinne der VVM - Gesamtmethode ist eine sprachlich und formal geordnete Darstellung einer Menge von Konzepten und deren Beziehungen innerhalb einer Domäne. Im VVM-Kontext wird die A.U.T.O. Ontologie verwendet. Sie integriert “Wissen über die Domäne”, das unter anderem aus Experten-Interviews und Kritikatitätsanalysen entsteht mit den Strukturen des Szenario-Modells. Aus Datenanalysen werden “Kritikalitätsphänomene” und “Wirkzusammenhänge” identifiziert und in der A.U.T.O. Ontologie in formaler Form mit den Beschreibungsstrukturen des Szenario-Modells zusammengeführt. (siehe auch Kapitel 3.1.1.6)

Warum brauchen wir ein szenariobasiertes ODD-Metamodell?

Im Rahmen des etablierten Entwicklungsprozesses werden Szenarien zur Formulierung von Anforderungen, zum Entwurf von Architekturen, Soft- und Hardwarekomponenten, zur Verifikation und Validierung des funktionalen Sicherheitskonzeptes sowie zur Verifikation und Validierung des integrierten Gesamtsystems im Testprozess eingesetzt. PEGASUS hat das szenariobasierte Testen für automatisierte Fahrsysteme etabliert und damit die szenariobasierte Bewertung des Restrisikos sowie die systematische, strukturierte Generierung von Testfällen mittels des 6-Ebenen-Szenarienmodells in den V&V-Prozess integriert.

Aufgrund der Anforderungen, die sich aus der Verwendung von Szenarien in den verschiedenen Entwicklungsphasen ergeben haben, wurden in den verschiedenen Entwicklungsphasen häufig unterschiedliche Szenariobegriffe und -beschreibungen verwendet.

Dies und die daraus resultierenden Brüche in den Beschreibungen und Abstraktionsebenen erschweren unter anderem

(1) nachzuweisen, dass die verwendeten Modelle ein hinreichend repräsentatives Abbild der (realen) ODD darstellen. Es ist nachzuweisen, dass die verwendeten Szenarioklassen und die im Szenario verwendeten beschreibenden Parameter die realen Szenarien in der adressierten Betriebsumgebung adäquat abdecken.

(2) einen durchgängigen, nachvollziehbaren und verifizierbaren Prozess des Requirements Engineering einschließlich dessen Verifizierung/Validierung zu etablieren

(3) nachzuweisen, dass die im Rahmen der V&V durchgeführten Tests und die Felddatenanalyse auf dem gleichen semantischen Datenmodell basieren, das zur Beschreibung der Szenarioklassen und -eigenschaften während der Problemanalyse und Systemspezifikation verwendet wurde (Gefahren und gefährliche Situationen, die systematisch in der ODD auftreten, wurden identifiziert und werden im Systemdesign mit einem akzeptablen Risiko behandelt).

Integration in den Entwicklungsprozess

Das ODD-Metamodell enthält sowohl die funktionalen als auch die logischen CORE-Szenarien. Durch Parametrisierung und Instanziierung können funktionale, logische und daraus abgeleitete konkrete Szenarien ineinander überführt werden. In der Abbildung 74 ist die Zuordnung der Detaillierungsebenen im V-Modell dargestellt. Die funktionalen Szenarien werden insbesondere im Rahmen der Systemspezifikation in der Domänen-/Problemanalyse verwendet, um die Anforderungen - insbesondere an ein sicheres, regel- und gesetzeskonformes Systemverhalten - an die automatisierte Fahrfunktion (ADF) für die Kritikalitäts- und Gefährdungsanalyse sowie die Risikobewertung zu spezifizieren. Technische Anforderungen können über die Instanziierung und ihre zugehörigen Randbedingungen durch Parametrisierung und Übertragung der sprachlichen bzw. visuellen Semantik in logische Szenario-Instanzen formuliert werden. Im Rahmen der Verifikation werden konkrete Szenarien als Input für die Durchführung von Tests benötigt. Hierzu werden aus den logischen Szenario-Instanzen mit Hilfe von Samplingverfahren konkrete Szenarien abgeleitet. Im Rahmen von Testspezifikationen werden sie bei der Anforderungsverifikation und Testzielverifikation geeigneten Testinstanzen zugeordnet und um Pass/Fail-Kriterien ergänzt. Szenarien definieren im Test Herausforderungen an das System, die der Verifikation dienen, inwieweit ADS bzw. ADF durch ihr implementiertes Verhalten die durch die Requirements definierten Sollvorgaben erfüllen. Das Testziel besteht darin, die Konformität des implementierten Verhaltens mit dem spezifizierten Verhalten nachzuweisen. Dies schließt das Erreichen der Leistungsziele ein. Dies entspricht der Überprüfung der Implementierung bzw. dem Aufzeigen einer Implementierungslücke.

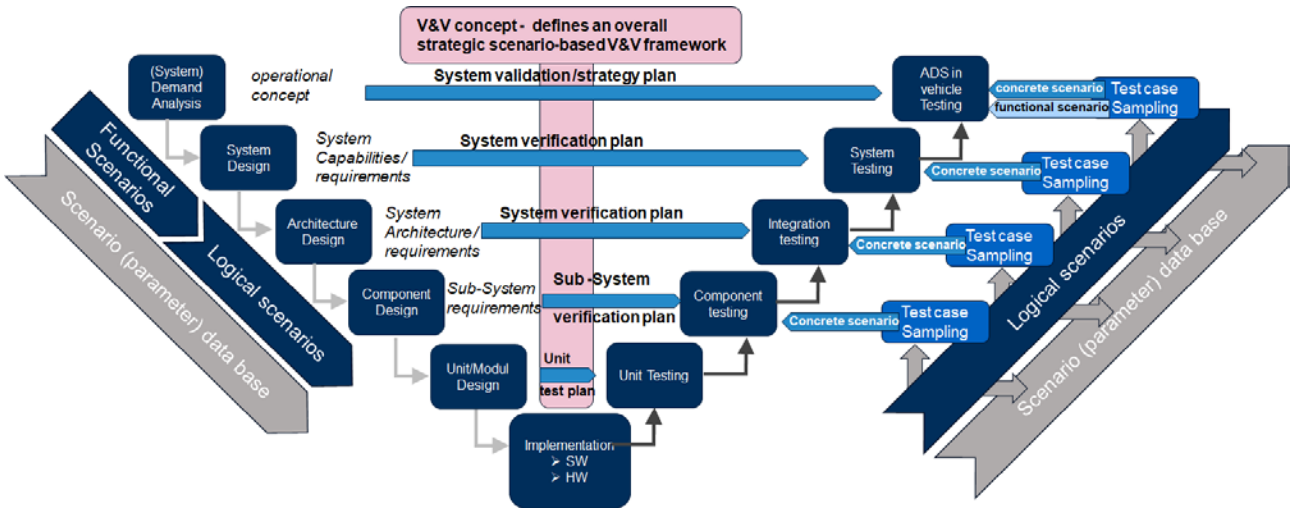


Abbildung 74: Nutzung des ODD- Metamodells (funktionale, logische CORE Szenarien, Szenario Datenbank) im Entwicklungsprozess (V-Modell)

Ausblick und Einordnung: die Rolle des Szenario-Konzeptes in der Gesamtmethode

Das ODD Metamodells spielt in der VVM-Gesamtmethode eine entscheidende Rolle. Abbildung 74 zeigt die Verwendung der unterschiedlichen Detaillierungslevel in den Prozessschritten des V-Modells von der Konzeptphase über die technische Entwicklung bis zur Verifikation und Validierung.

Die CORE Szenarien beschreiben (siehe Abbildung 75)

- den Entwicklungsraum,
- den Testraum und
- das Datenmodel für Betriebsdomäne und KPI´s des zu entwickelnden automatischen Fahrsystems.

Die Szenariodatenbank liefert ein statistisches Abbild der Betriebsdomäne, das an vielen Stellen im Prozess genutzt wird. Beispiele sind die Instanziierung der Szenarien mit validen Wertebereichen, die gezielte Steuerung von Methoden in die risikobehafteten bzw. den Bereichen des risikoarmen Fahrens.

In der Konzept- und Entwicklungsphase dienen Szenarien zur Spezifikation des Entwicklungsgegenstandes ADS, der Analyse der Betriebssituationen und -Zustände und der Spezifikation von risikoakzeptablem und -konformem, funktionalem Verhalten und korrespondierenden Systemarchitekturen (Siehe Abbildung 75).

> Aus Prozesssicht ist das ODD Metamodell, das hinreichend vollständig die ODD repräsentiert (siehe Kapitel 3.1.1.4.5.2), ein essentieller Bestandteil, um einen durchgängigen, nachvollziehbaren und überprüfbaren Prozess zur (nahezu vollständigen) Ableitung von Requirements zu etablieren. Dies trägt bei zum Schließen der Spezifikationslücke.

In der Verifikation & Validierung dienen Szenarien (siehe Abbildung 75) dazu, zu überprüfen ob das implementierte ADS die in der technischen Entwicklung definierten Requirements erfüllt. Im Rahmen der Verifikation wird dies durch systematisches Testen evaluiert. Die CORE Szenarien spannen den Testraum auf, sie sind ein hinreichend vollständiges Modell für die zu erwartenden Betriebssituationen und Betriebsbedingungen, in denen das integrierte ADS regel-konform, mit akzeptablem Risiko operieren muss.

> In der Verifikation wird systematisch anhand des Testkonzeptes mit Testfallspezifikationen aus den Szenario-Instanzen das dynamisches Verhalten von Objekten und die Umgebungsbedingungen in den gültigen Wertebereichen variiert und so konkrete Testszenarien erzeugt. In ihnen wird das durch die Anforderungen definierte Sollverhalten im Rahmen der Testziele überprüft.
>
> In der Validierung dienen die Szenario-Klassen dazu, die Abdeckung des Testraumes durch Testfahrten zu überwachen und die Test zur Überprüfung der Validierungsziele im Rahmen des Validierungskonzeptes durchzuführen.
>
> Aus Prozesssicht ist das ODD Metamodell, das hinreichend vollständig die ODD repräsentiert, ein essentieller Bestandteil, um einen durchgängigen, nachvollziehbaren und

überprüfbaren Prozess zur (nahezu vollständigen) Überprüfung von Requirements zu etablieren sowie Testziele und Validierung durchzuführen. Dies trägt bei zum Schließen der Implementierungslücke.

Abbildung 75 zeigt einen dritten Block: die Felddatenerhebung bzw. die Felddatenanalyse. Hier dienen die CORE Szenario-Klassen als Klassifikatoren von im Realverkehr erhobenen Messdaten. Der Datenpool stellt den Abgleich des ODD-Modells gegenüber der ODD-Realität bzw. auftretenden Betriebssituationen und -zuständen und notwendiger Performanz dar. Die Daten fließen sowohl in die Entwicklung als auch das V&V ein.

Aus Prozesssicht ist mit der Felddatenerhebung / -analyse der Kreis zwischen durchgängiger Verwendung des ODD-Metamodells in Entwicklung und Absicherung durch einen Abgleich mit den realen Betriebssituationen und -zuständen in der ODD abgeschlossen. Sowohl die Tests als auch die Felddatenanalyse beruhen auf demselben semantischen Datenmodell, das zur Beschreibung der CORE Szenario-Klassen und Eigenschaften während der Spezifikation des Entwicklungsgegenstandes ADS, der Analyse der Betriebssituationen und -Zustände und Ableitung der Requirements im Rahmen der Konzept- und Entwicklungsphase benutzt wurde. Der Szenarienkreislauf stellt somit einen durchgängigen, nachverfolgbaren und überprüfbaren Prozess dar, ein hinreichend vollständiges Modell der ODD zu erstellen, mit der realen ODD abzugleichen und einheitlich bei der Entwicklung und Absicherung zu verwenden.

Sowohl die Tests als auch die Felddatenanalyse beruhen auf demselben semantischen Datenmodell zur Beschreibung der der Szenarioklassen und -eigenschaften während der Domänenanalyse

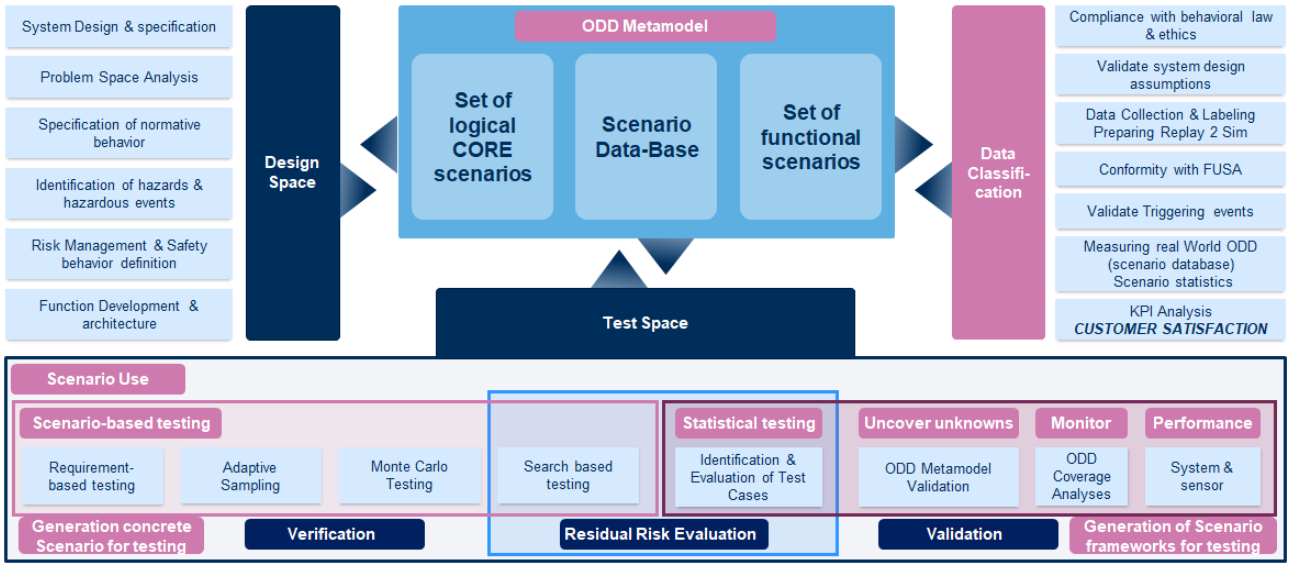


Abbildung 75: Die Rolle der CORE-Szenarien in der Gesamtmethode

Abbildung 75 veranschaulicht die Prozesse, die auf die Szenarienräume (Entwicklungsraum, Testraum, Felddatenraum) einwirken. Das ODD-Metamodell stellt die grundlegenden Strukturen bereit, auf denen die Prozesse der Entwicklung, Validierung und Datenerhebung arbeiten. Die Prozesse stellen Integritätsanforderungen an das ODD-Metamodell, die zu Modellanpassungen führen, wie z.B. zusätzliche CORE-Szenarioinstanzen und Datenabgleich. Abbildung 71 zeigt, dass die gesamte VVM-Methodik einen besonderen Schwerpunkt auf die durchgängige

Verwendung von Szenariomodellen legt und dass diese die reale ODD hinreichend zutreffend abbilden. Notwendige Nachweise, die in die (sicherheitstechnische) Argumentation einfließen, sind die Verifikationsergebnisse, die Bewertung des Restrisikos und die Validierungsergebnisse (siehe Kapitel Szenarienabstraktion Grundlagen (Realitätsabstraktion)3.1.1.4).

Rolle des ODD Metamodells im Safety Case

Die VVM-Gesamtmethode besteht aus zwei sich ergänzenden, parallelen Prozessen, dem Szenarien-Prozess und dem Entwicklungs- und Absicherungsprozess. (siehe Abbildung 76)

Der Szenarienprozess stellt der Entwicklungs- und Absicherungsprozess ein valides Modell für die ODD zur Verfügung. Durch den Szenarienprozess werden die “unknow” über die ODD reduziert. Das ODD Metamodell trägt dazu bei, dass die Ableitung von Anforderungen an das ADS (vollständig in dem Sinne von der Schaffung der Voraussetzungen) erreicht werden kann.

Dadurch kann eine Erhöhung der Robustheit des ADS gegenüber Gefährdungen und gefährlichen Situationen in dem bestimmungsgemäßen Einsatzbereich mit seinen spezifischen Betriebsbedingungen durch die systematische Suche und Integration bisher nicht im ODD-Metamodell berücksichtigten CORE-Szenarien und ODD- bzw. Szenario-Merkmalen erreicht werden.

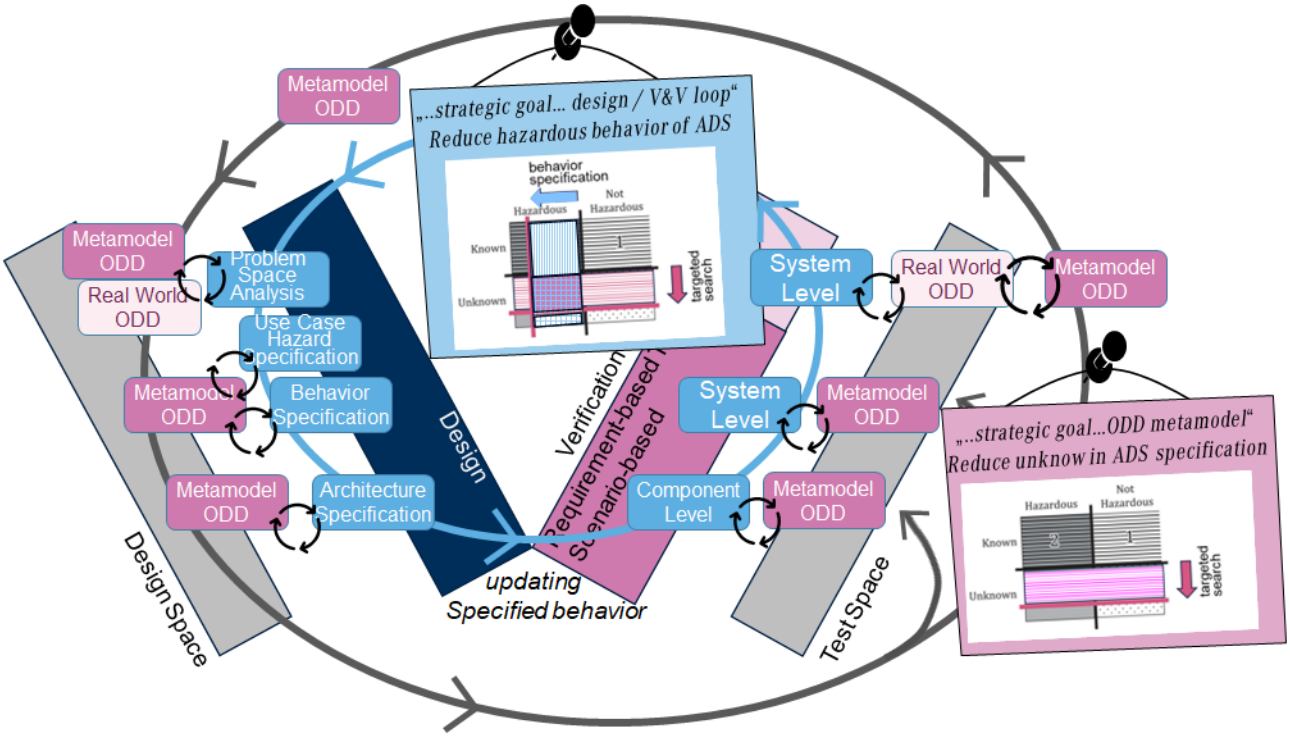


Abbildung 76: Interdependente Reduktion von “gefährlichem Systemverhalten” (adaptierte Methoden im V-Modell) und “ bisher unbekannten Anforderungen aus ODD” (Adaption Entwicklungs- und Testraum ODD-Metamodell)

Hierauf wird im Verlauf des Abschnitts detailliert eingegangen:

Von Daten zu logischen Szenarien mit Parameterverteilungen

Bei der Entwicklung eines szenariobasierten Metamodells für ODD werden funktionale oder logische Szenarien (Klassen) erstellt. Der nächste Schritt ist die Festlegung von Wertebereichen für die ausgewählten Parameter. Dies kann auf der Basis von Expertenwissen erfolgen. Es können aber auch repräsentative reale Verkehrsdaten verwendet werden. Um automatisierte Algorithmen anwenden zu können, muss ein gemeinsames Datenformat für Trajektorien- und Kartendaten zur Verfügung stehen. Mit diesen Werkzeugen werden Datensequenzen, die zu Szenarien passen, identifiziert und den entsprechenden Szenarien zugeordnet, was zu Verteilungen von Parametern und Attributen führt.

Datenbank mit logischen Stadtverkehrsszenarien die systematisches Testen des ODD ermöglichen

Der Zweck einer Szenariendatenbank besteht darin, die reale Welt des OD zu repräsentieren. Das (holistische) Szenariokonzept zusammen mit beschreibenden Parametern ist der Schlüssel zu einer solchen Repräsentation.

Datenbasierte Identifikation von Szenarien mit hohem Risiko

Alternativ zu unserem konstruktiven ganzheitlichen Szenarioansatz kann für den speziellen Fall, dass das ADS in einer ODD zwischen festen Haltestellen verkehrt, auch ein pragmatischer Ansatz gewählt werden. Der erste Schritt ist die Definition von Trajektorien für alle möglichen Verbindungen. Merkmale, wie z. B. grundlegende Manöver und deren Gefährlichkeit, werden in diesen Trajektorien identifiziert. In Kombination mit dem Schweregrad und der Gefährdung, die aus Unfalldatenbanken entnommen werden, ergeben sich funktionale Szenarien mit hohem Risiko, die im Entwicklungsprozess verwendet und weiter qualifiziert werden können.

3.1.1.4.2 Ganzheitliches urbanes Fahrszenario-Konzept

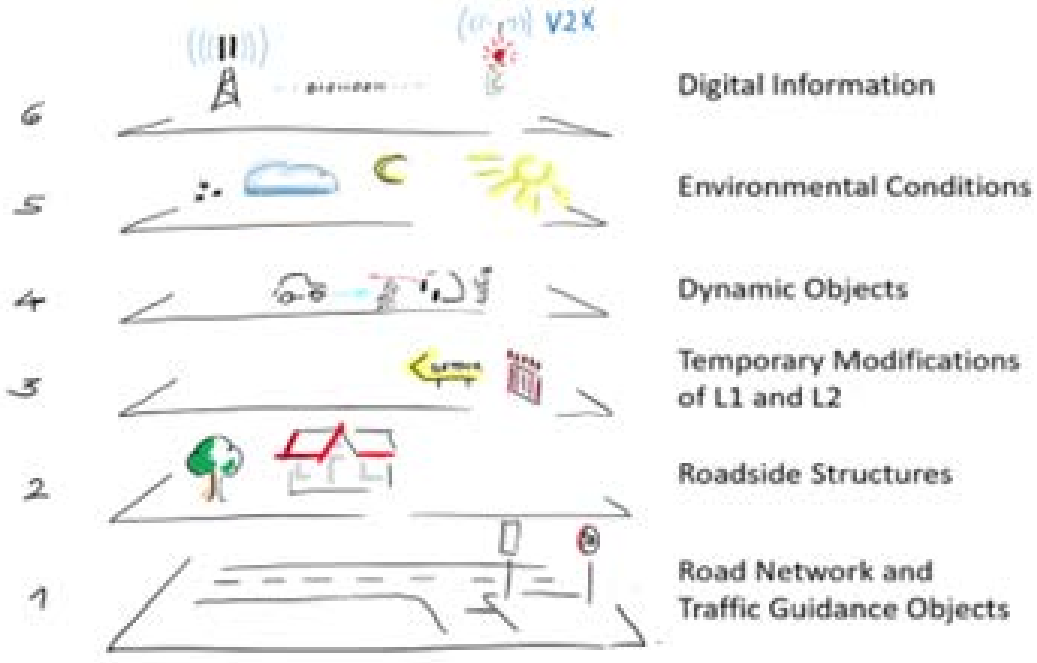


Abbildung 77: Abbildung 05.02.01: 6-Ebenen-Modell [46]

Für die Validierung und Verifizierung automatisierter Fahrfunktionen durch szenariobasiertes Testen muss das in der ODD auftretende Verkehrsgeschehen über Szenarien dargestellt werden.

Um dies zu erreichen, wird in VVM eine systematische Ableitung einer Gruppe von Szenarien, die die ODD abdecken, vorgenommen. Der Regelsatz nach dem diese Ableitung stattfindet, wird Szenarienkonzept genannt. In VVM bildet das 6-Ebenen-Modell die Grundlage des Szenarienkonzepts und der aufgebauten Ontologie A.U.T.O. Das 6-Ebenen-Modell strukturiert das Verkehrsgeschehen in sechs Ebenen, welche in der untenstehenden Grafik zu sehen sind.

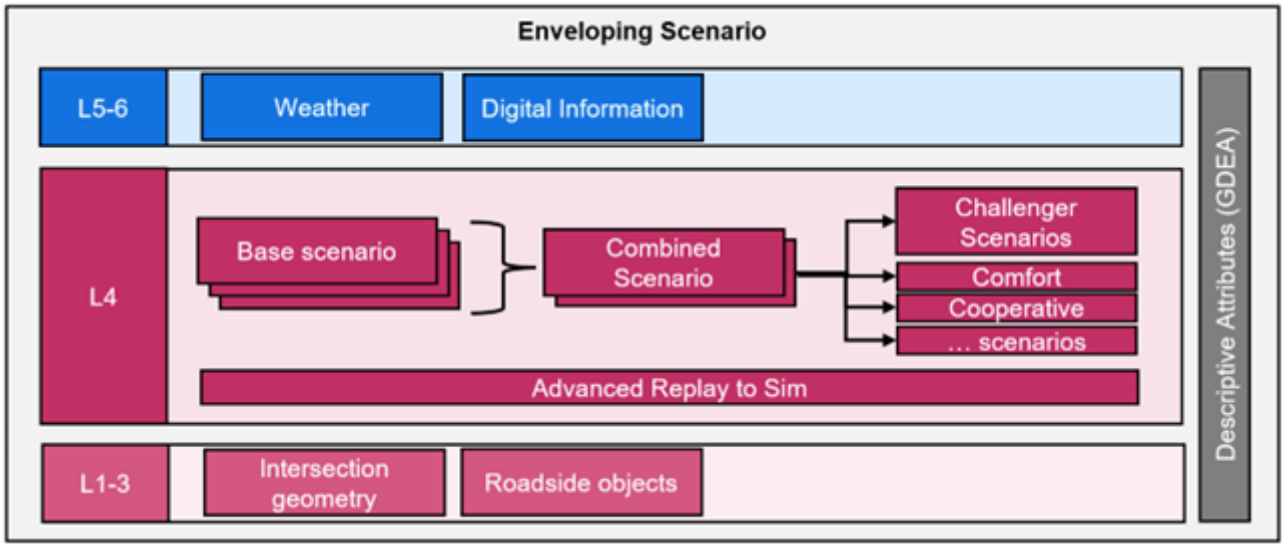


Abbildung 78: Szenarienkonzept [60]

Entsprechend dieser Struktur, ergeben sich für das Szenarienkonzept drei Beschreibungsbereiche: die Beschreibung der Straße und Umgebung (Ebene 1-3), der dynamischen Objekte und ihren Beziehungen (Ebene 4) und der Umwelteinflüsse und digitalen Informationen (Ebene 5 und 6) (siehe Abbildung 78). Im ersten Schritt des Szenarienkonzepts wird die Perspektive eines Verkehrsteilnehmers (dem Ego) gewählt und das Verkehrsgeschehen aus dessen Perspektive in Abschnitten des Verkehrsraums (z.B., Kreuzung, Straße, Kreisverkehr, Autobahnstück, Autobahnauffahrt) beschrieben, was als Enveloping Scenario bezeichnet wird.

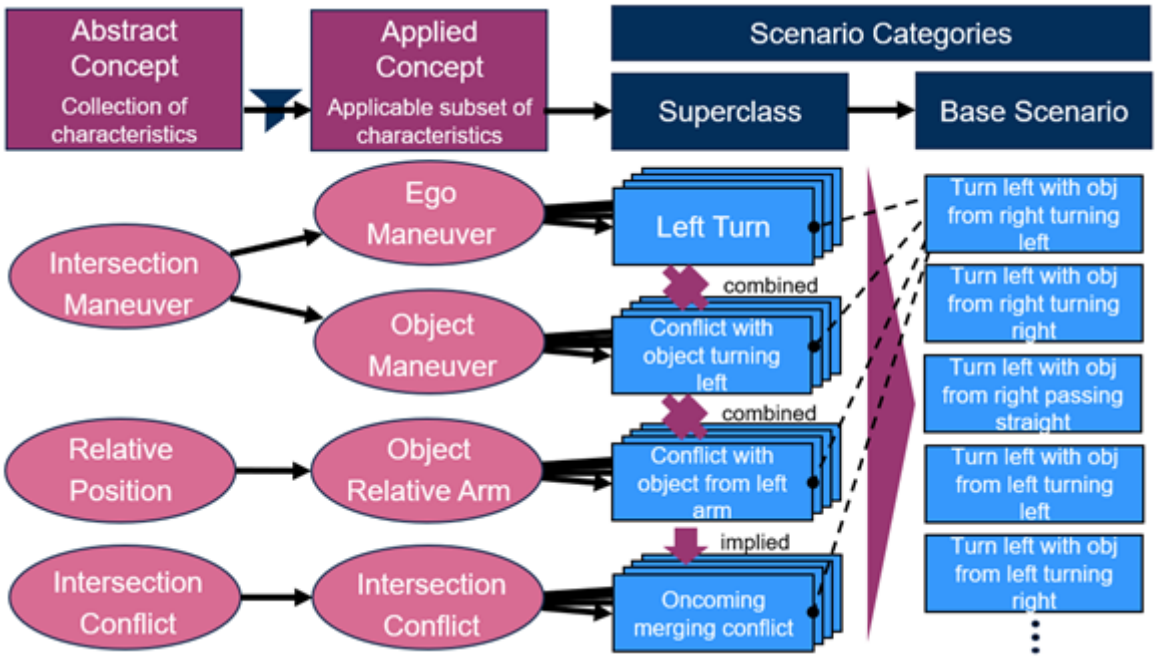


Abbildung 79: Basis Szenarien (Base Scenario) aus Kombination von Konzepten [60]

Eine besondere Herausforderung in der Ableitung von Szenarien ist die Beschreibung der Dynamiken und Interaktionen von Verkehrsteilnehmern. Um die Komplexität zu reduzieren, werden die verschiedenen Aspekte der Verkehrsdynamiken einzeln durch sogenannte Konzepte beschrieben. Beispiele sind das Kreuzungs-Manöver des Ego-Fahrzeuges und die Art des Kreuzungskonflikts zweier Verkehrsteilnehmer. Diese Konzepte lassen sich in drei Kategorien einteilen:

- Individuelle Konzepte betreffen nur das Ego-Fahrzeug.
- Bilaterale Konzepte betreffen die Interaktion von Ego-Fahrzeug und genau einem Verkehrsteilnehmer.
- Globale Konzepte betreffen die Verkehrsart und Umgebung.

Durch die Kombination dieser Konzepte lassen sich systematisch Basis-Szenarien (base scenario) definieren. Vorteil dieses Vorgehens ist die Reduzierung der Komplexität des Verkehrsgeschehens durch Ausnutzung von Kombinatorik. Dies vereinfacht insbesondere die Szenarien-Identifizierung, Generierung und Ausspielung in die Simulation. Die Konzepte, deren Typen und Kombinationsmöglichkeiten werden in einer Ontologie festgehalten. Dies hilft, eine Argumentation mit dem Szenarienkonzept und anderen Bestandteilen der Methodik zu verknüpfen. Ebenfalls wird dadurch die Kombinatorik durchgeführt und explizit dokumentiert. Der so erzeugte Satz an Basisszenarien umfasst weniger als 300 Szenarien.

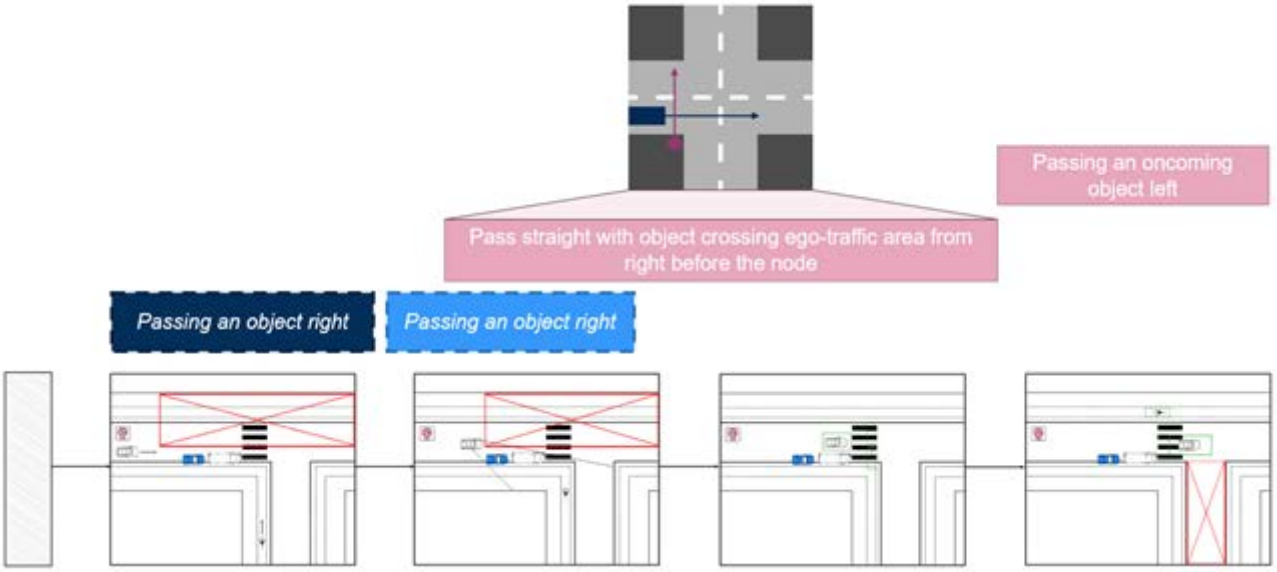


Abbildung 80: Zusammensetzung von Verkehrsgeschehen aus Basis Szenarien als Bausteine [60]

Die Basis-Szenarien können als Bausteine verstanden werden, aus denen längere und komplexere Verkehrsgeschehen zusammengesetzt werden (siehe Abbildung 80). Solche Kombinationen werden als Kombinierte-Szenarien bezeichnet. Bei der Kombinierung können Basis-Szenarien sowohl sequenziell als auch parallel ablaufen.

3.1.1.4.3 Von Daten zu logischen Szenarien mit Parameterverteilungen

Ein Szenario kann in verschiedenen Abstraktionsstufen beschrieben werden. Für das Folgende sind zwei Stufen relevant: das konkrete Szenario und das logische Szenario. Das logische Szenario beschreibt eine Situation mithilfe von Parametern, die deren gültigen Wertebereich beschreiben. Eine Variation dieser Paramater erzeugt also eine Variation des Szenarios. Grenzwerte der Parameter und Abhängigkeiten unter den Parametern sind auch Teil des Logischen Szenarios. Sind zu den Parametern des Logischen Szenario zusätzlich deren Verteilungen gegeben, wird dies als Logische Szenarien-Instanz bezeichnet. Dementgegen stellt ein konkretes Szenario nur eine einzige Verkehrssituation dar. Es kann durch Setzen der Parameter eines Logischen Szenarios auf feste Werte erzeugt werden.

Zwischenziel der VVM Methodik ist es Logische Szenario-Instanzen zu definieren welche systematisch getestet werden können. Hierzu müssen zu den Szenarien des Szenarienkonzepts Parameter definiert werden. Dazu wird die Eigenschaft der Basisszenarien benutzt, dass diese aus Konzepten kombiniert sind. Dementsprechend können für jedes Konzept getrennt Parameter definiert werden. Durch die Kombination der Parameter der Konzepte ergeben sich die Parameter der Basisszenarien, analog zur Definition der Szenarien selbst. Neben Parametern, welche zur Ausspielung in z.B. die Simulation genutzt werden, können nach vergleichbarem Vorgehen Attribute bestimmt werden, welche lediglich eine beschreibende Aufgabe erfüllen, aber nicht zwingend in die Ausspielung übertragbar sind. Diese sind vor allem bei der Identifizierung von Szenarien in Verkehrsdaten von Relevanz und verstärken die Filterungsmöglichkeiten in der Suche nach spezifischen Szenarien. Parameter und Attribute können z.B. aus der Kritikalitätsanalyse abgeleitet werden. Somit kann ein Satz logischer Szenarien erzeugt werden.

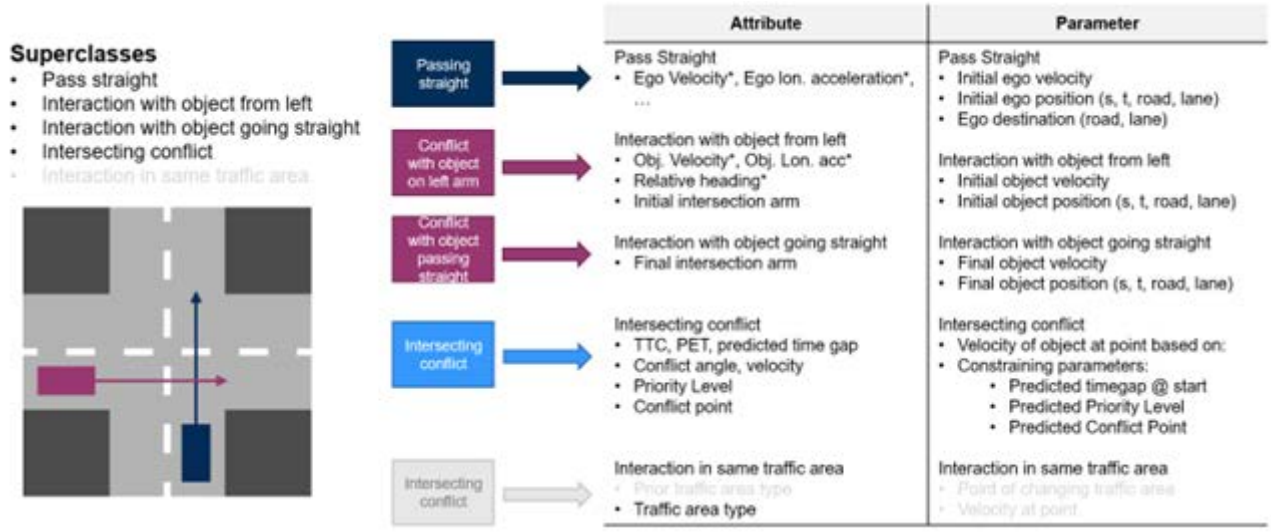


Abbildung 81: Beispielhafte Parameter-Definition der Basis-Szenarien aus Kombination der Konzepte (Superclasses) [60]

Um Logische Szenario-Instanzen zu erhalten, wird die Verteilung der Parameter benötigt. Um eine Abschätzung des Risikos in späteren Schritten der Methodik zu ermöglichen, sollten diese Verteilungen dem realen Auftreten des Parameters in der ODD entsprechen. Dazu muss tatsächlich auftretender Verkehr analysiert werden. Dazu werden in Messdaten durch Algorithmen Verkehrsszenarien identifiziert und die dazugehörigen Parameter und Attribute bestimmt. Hier zahlt sich erneut die Komposition von Basis-Szenarien aus Konzepten aus, da es signifikant die Anzahl an benötigter Logik reduziert. Wird so eine Menge an Szenarien und deren Parameter identifiziert, lassen sich die zugrundeliegende Verteilung und die Beziehungen der Parameter approximieren. Dazu eigenen sich z.B. Hybride Graphen. Somit können Logische Szenarien-Instanzen bestimmt werden.

3.1.1.4.4 Datenbank mit logischen Stadtverkehrsszenarien

Wie im vorangegangenen Abschnitt erwähnt, sollten die approximierten Verteilungen dem realen Auftreten der Szenarien in der ODD entsprechen. Neben Szenarien aus Wissensquellen, benötigt es dazu eine große und umfangreiche Menge an Verkehrsdaten und eine automatisierte Verarbeitung dieser. Das Verarbeiten und Managen der resultierenden Szenarien kann eine Szenariodatenbank übernehmen. Diese kümmert sich um das Verwalten der Eingangsdaten, um die Identifikation der Szenarien und deren Parameter und Attribute. Aus den in der Datenbank liegenden konkreten Szenarien erzeugt die Datenbank Logische Szenario-Instanzen und bietet Analysewerkzeuge für den Anwender. Des Weiteren bietet die Szenariendatenbank Möglichkeiten zum Filtern der Szenarien nach für den Use Case des Anwenders relevanten Merkmalen bzw. Kategorien und stellt aus den Szenarien abgeleitete Simulations-Szenarien in Form von OpenSCENARIO XML bereit.

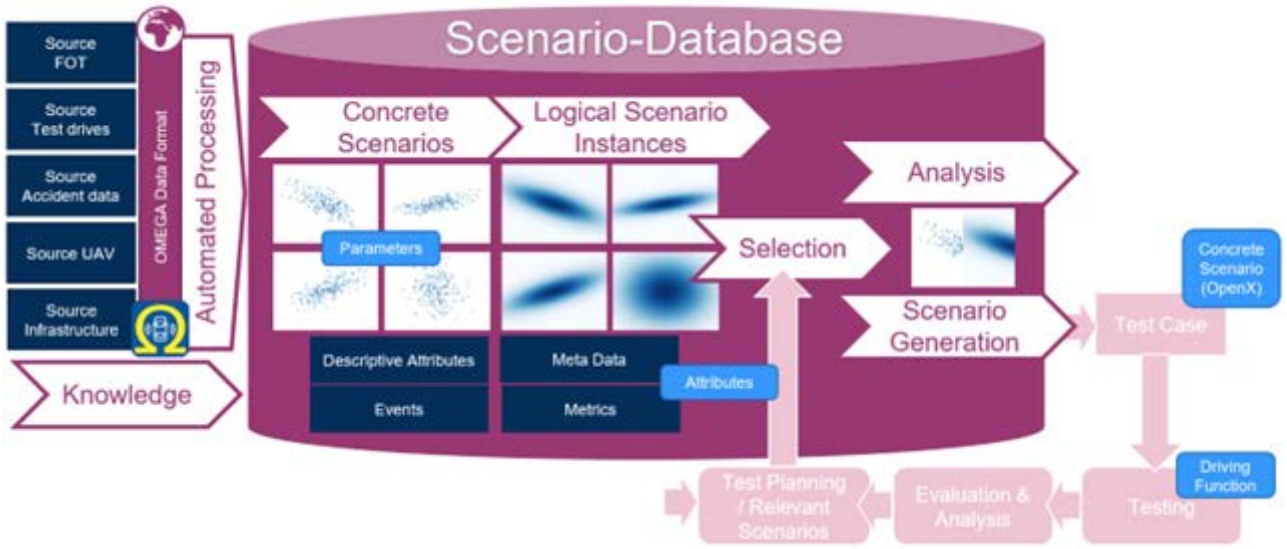


Abbildung 82: Aufbau der Szenariodatenbank

Um Daten aus verschiedenen Quellen automatisiert verarbeiten zu können, benötigt es einer Schnittstelle. In VVM wurde dazu das OMEGA-Format definiert. Es ist ein hierarchisches Datenformat, welches Informationen von allen 6 Ebenen des 6-Ebenen-Modells umfasst und zur A.U.T.O Ontologie übersetzbar ist. Es umfasst objektlistenbasierte Trajektorieninformationen von Verkehrsteilnehmern und Karten-Informationen angelehnt an das Lanelet2 Format. Das Format wurde aus dem PEGASUS-Datenformat und dem Common Data Format des EU Projektes L3Pilot entwickelt und an die Bedürfnisse des urbanen Use-Cases angepasst. Wichtigstes Merkmal ist die Verfügbarkeit von Konvertern, die eine Aufnahme von Daten verschiedenster etablierter Formate in die Szenario-Datenbank ermöglichen.

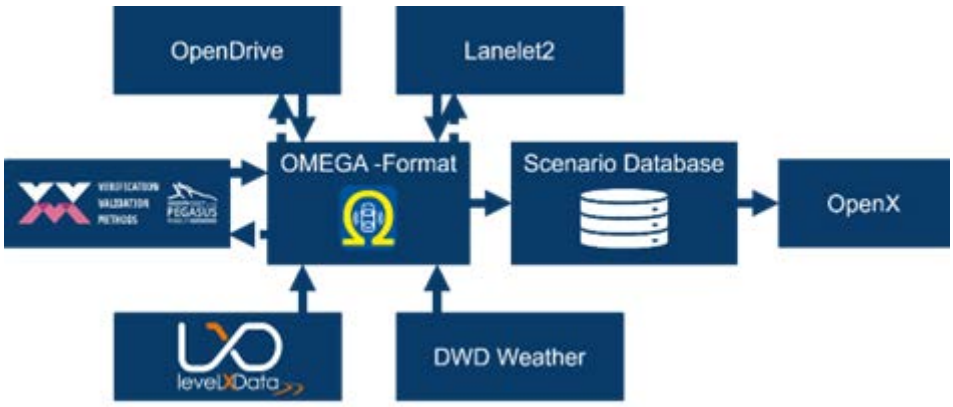


Abbildung 83: Das OMEGA-Format als Schnittstelle zwischen Datenquellen und Szenario-Datenbank [60]

Somit ermöglicht die vorgestellte Methodik die Komplexität des realen Verkehrs durch ein Szenarienkonzept und die Funktionalitäten der Szenarien-Datenbank in testbare und simulierbare Logische Szenarien-Instanzen zu übersetzen.

3.1.1.4.5 Vorgehen zur Vollständigkeitsargumentation des Szenario Konzepts

Ein umfassendes Verständnis der operativen Domäne (OD) ist der Schlüssel zu automatisierten Fahrsystemen (ADS). Unser Verständnis über die OD wird in Form von Szenarien beschrieben.

Die Vollständigkeit solcher Szenarien hängt zum einen von der Vollständigkeit des Konzepts ab, mit dem Szenarien spezifiziert werden, und zum anderen davon, ob Szenarien spezifiziert wurden, die der OD ähneln. Wir konzentrieren uns hier ausschließlich auf den ersteren Punkt und zeigen, wie Argumentationstechniken zur Vollständigkeit des Szenariokonzepts beitragen können.

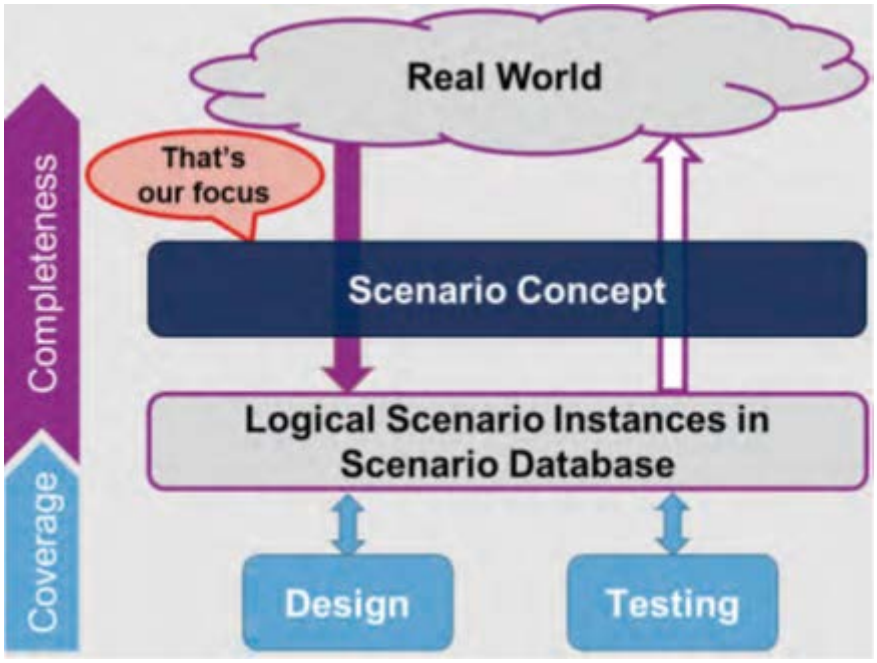


Abbildung 84: Beziehung zwischen der realen Welt, dem Szenariokonzept und der Szenariodatenbank. Der violette Pfeil illustriert den Fokus dieses Beitrages, welcher sich mit der Vollständigkeit des Szenariokonzepts befasst.

3.1.1.4.5.1 Das Verfahren

Die Vollständigkeitsargumentation gliedert sich in die Argumentation der Konsistenz des Szenariokonzepts (siehe Abbildung 85) gefolgt von dessen Vollständigkeit (siehe Abbildung 86). Interessanterweise dienen die in Abbildung 85 gezeigten GSN-Strategien als Startpunkt für die Vollständigkeitsargumentation. Dies liegt daran, dass ein Fehlen von Unterzielen (Ziele, die einer Strategie folgen) eine Strategie als ungültig und damit als unvollständig darstellen würde.

Da wir nicht wissen können, was unbekannt ist, wird ein Gegenargument formuliert, das die Vollständigkeit jeder Strategie hypothetisch in Frage stellt. Typischerweise kann eine Hypothese entweder akzeptiert oder abgelehnt werden. Im Falle eines ADS kann es auch beides sein, was zu einem Dilemma führt. Gründe dafür können unbekannte Unbekannte oder ein nicht spezifizierter Kontext sein. Beide Gründe lassen sich mittels unserer entwickelten Pattern (siehe Abbildung 86) adressieren.

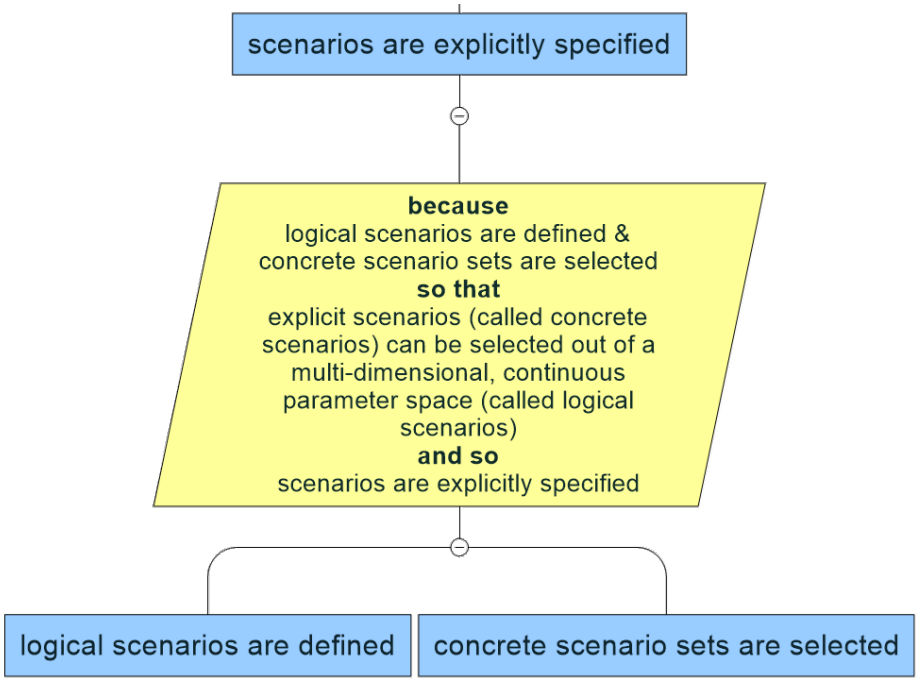


Abbildung 85: Claim „scenarios are explicitly specified" (oben in Blau) im Zusammenspiel mit der Strategie (in Gelb dargestellt) zur Anbindung der zwei sub-claims (unten in Blau) in Goal Structuring Notation (GSN) dargestellt.

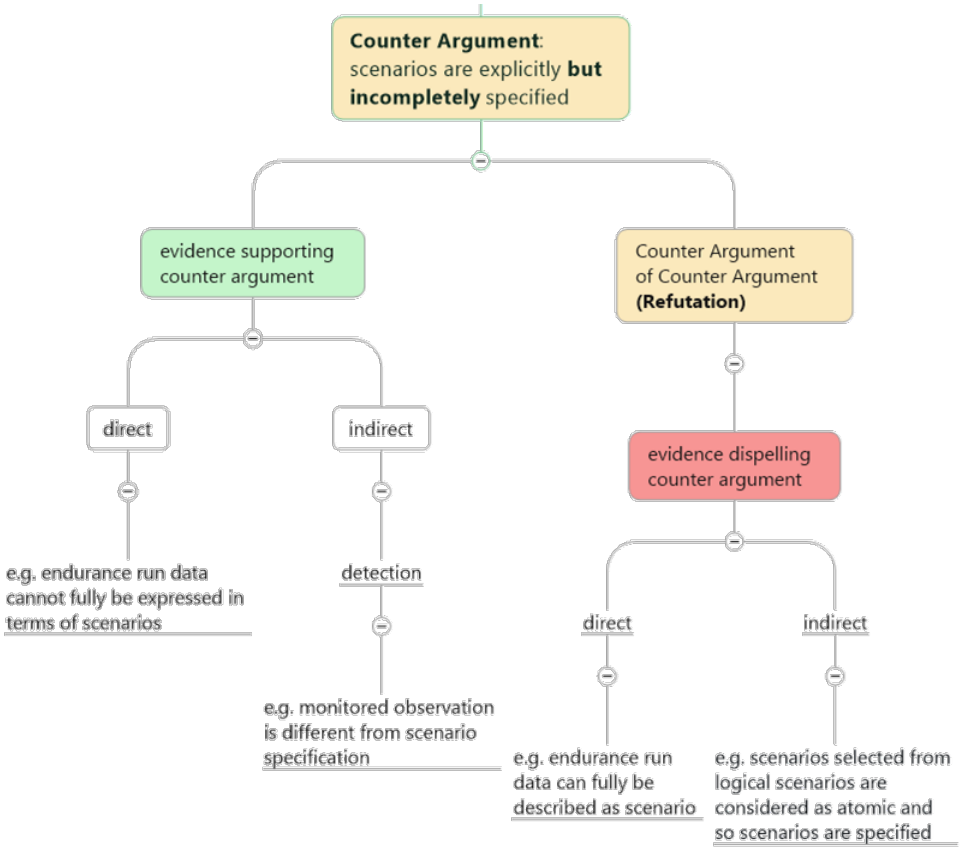


Abbildung 86: Gegenargument für die in Abbildung 85 gezeigte Strategie, wobei die linke Seite die Nachweise zeigt, welche das Gegenargument stützen, und die rechte Seite die Nachweise gruppiert, um das Gegenargument auszuräumen (©Robert Bosch GmbH).

3.1.1.4.5.2 Vollständigkeitsargumentation

Wie in Abbildung 86 dargestellt, wird jede Strategie durch ein Gegenargument als Hypothese für die potenzielle Unvollständigkeit der argumentierten Strategie in Frage gestellt. Im Falle einer akzeptierten Hypothese haben wir Nachweise für die Unvollständigkeit der Strategie gefunden. Infolgedessen müssten dann die jeweiligen Teilziele entsprechend erweitert und somit angepasst werden. Im Gegensatz dazu bedeutet eine abgelehnte Hypothese, dass wir nicht in der Lage waren, Nachweise für das Gegenargument zu liefern, so dass die jeweilige Strategie als vollständig angesehen werden kann. Der Fall eines Widerspruchs aufgrund einer akzeptierten und einer abgelehnten Hypothese bedeutet, dass weitere Kenntnisse über den Kontext notwendig sind, um den Widerspruch aufzulösen.

3.1.1.4.6 Ontologie und OD Beschreibung

Eine grundlegende Annahme in der VVM-Gesamtmethode ist die Verfügbarkeit einer (formalen) OD-Beschreibung. Hier stellen sich folgende Fragen:

- Welche Werkzeuge können zum Beschreiben und Formalisieren der OD genutzt werden?
- Was sind mögliche Dekompositionen der OD und welche davon soll für die Beschreibung genutzt werden?
- Was sind die sicherheitsrelevanten Faktoren in der OD?

In VVM wurden für diese Fragen Ontologien als zentrales Werkzeug benutzt. Diese ermöglichen Nutzern ihre Konzeptualisierung einer Domäne (hier: Verkehr) zu formalisieren. Idealerweise geschieht dies in einem kollaborativen Prozess zwischen allen Stakeholdern.

Folgendes Beispiel demonstriert die Relevanz von Ontologien für die OD-Beschreibung, wenn mehrere Stakeholder beteiligt sind:

Die StVZO definiert nichtmotorisierte Transportmittel mit einer Maximalgeschwindigkeit von 6 km/h nicht als Fahrzeug (z.B. Kinderfahrräder). Diese Klassifizierung hat jedoch Implikationen für das System (bspw. Anforderungen) und muss somit nachverfolgbar niedergeschrieben werden.

Somit formen Ontologien die Basis einer OD-Beschreibung. Um Ontologien zu beschreiben, wurde in VVM mit der Web Ontology Language (OWL) ein etablierter Mechanismus genutzt. Abbildung 87 zeigt die in VVM entwickelte, zentrale Automotive Urban Traffic Ontology (A.U.T.O.). Diese kann als Basis für OD-Beschreibungen genutzt werden.

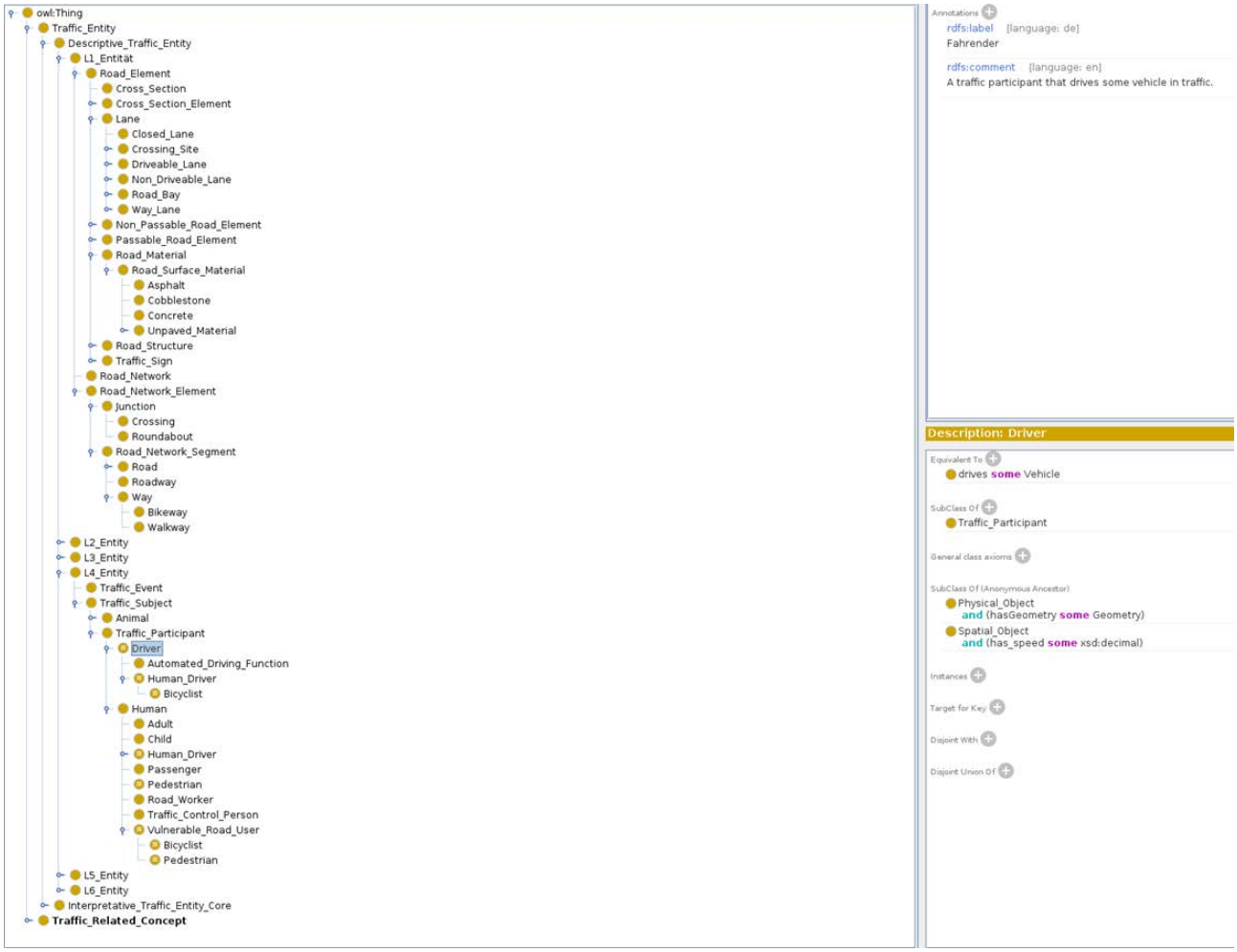


Abbildung 87: Die Automotive Urban Traffic Ontology (A.U.T.O.) mit logischen Axiomen im Protégé Editor

Als Folgefrage stellt sich nun die Aufgabe der Ontologieerstellung: Welche Klassen sollte man wählen, welche logischen Verbindungen sind relevant? Die in VVM entwickelte Idee ist es, den Prozess der Ontologieerstellung in den Prozess der Formalisierung von Kritikalitätsphänomenen zu integrieren.

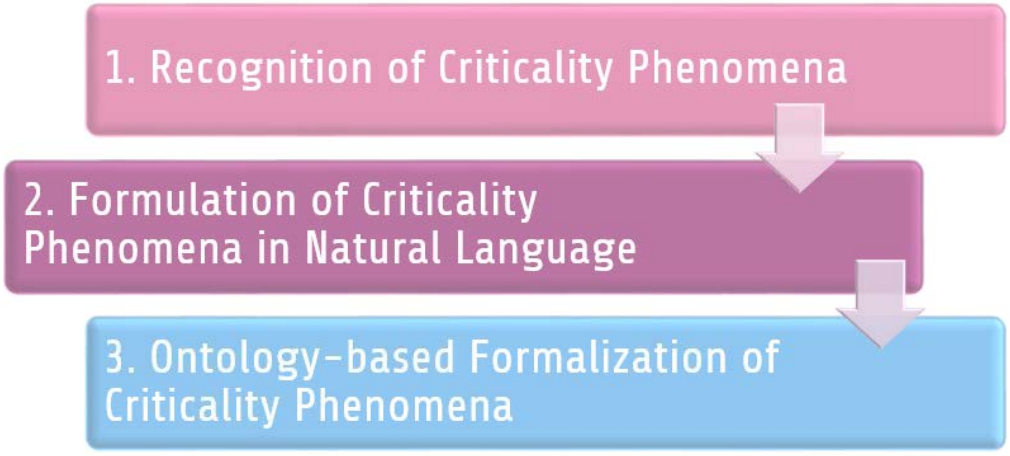


Abbildung 88: Prozess zur Formalisierung von Kritikalitätsphänomenen [61]

Der Prozess erzeugt einen Katalog von formalisierten Kritikalitätsphänomenen. Die zugrundeliegende Formalisierung erfolgt ebenso ontologiebasiert, weshalb die in Schritt 3 entstandene Ontologie wieder benutzt werden kann. Eines der Zwischenergebnisse dieses Prozesses ist ein Netzwerk an Kritikalitätsphänomenen.

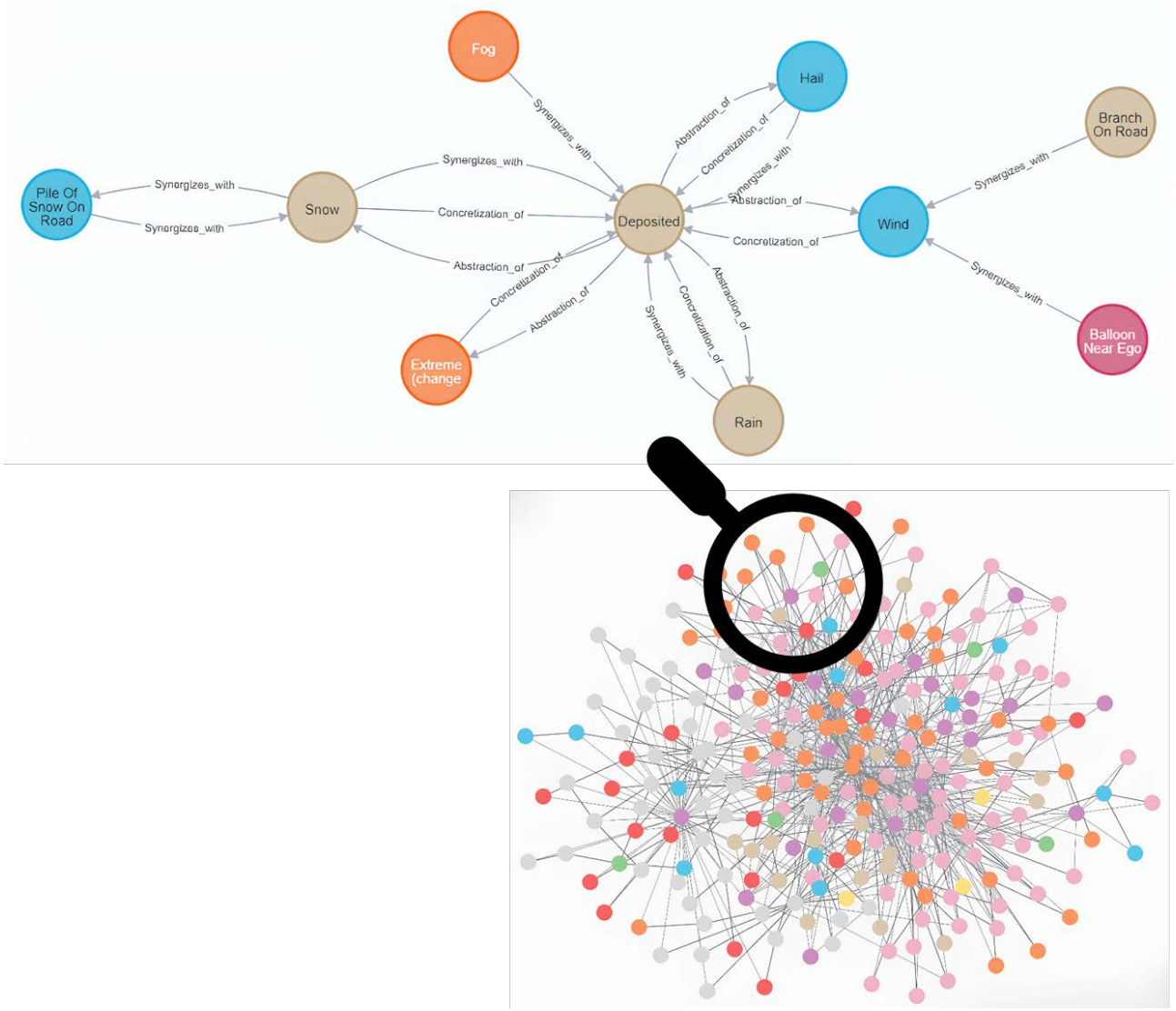


Abbildung 89: Netzwerk an Kritikalitätsphänomenen und ihre Relationen. Dieses ist noch nicht die hinter den Kritikalitätsphänomenen liegende Ontologie, es ist jedoch ein erster Schritt zu dieser.

In diesem Netzwerk an Kritikalitätsphänomenen ist jedes Phänomen mit einer natürlichsprachigen Definition versehen (Schritt 2). Diese Definition kann nun genommen, in sprachliche Komponenten zerlegt und letztendlich ontologisch formalisiert werden.

Ein Beispiel dieses Prozesses kann wie folgt aussehen:

Natürlichsprachige Definition eines Kritikalitätsphänomens:

Schritt 2 im Prozess ergibt folgende Definition: “Starkregen” ist ein Regen mit einer Intensität von mindestens 20 mm/h.

Wir erweitern nun unsere Ontologie wie folgt:

- Hinzufügen einer Klasse “Regen”
- Hinzufügen eines Attributs zur Klasse “Regen”: “Intensität in mm/h”
- Hinzufügen eines Attributs zur Klasse “Umgebung”: “hat Regen”

Sobald eine Ontologie formal definiert ist, kann diese wiederverfolgbar und präzise als Grundlage für die OD-Beschreibung dienen und als formales Werkzeug in weiteren Schritten der Absicherung eingesetzt sowie bspw. zur formalen Datenanalyse [62] genutzt werden.

3.1.1.4.7 Datenbasierte Identifikation von risikobehafteten Szenarien

3.1.1.4.8 Motivation

Die hier vorgestellte Methode erzeugt sicherheitsrelevante Testfälle und priorisiert sie nach risikobehafteten Szenariomerkmalen der möglichen Routen, die ein ADS in einem Geofence zwischen fixen Haltepunkten anfahren kann. Durch das priorisierte und gezielte Testen risikoreicher Fälle wird es ermöglicht, den Testraum für eine Verifikation bzw. Validierung auf Gesamtsystemebene deutlich zu reduzieren. Somit wird ein Beitrag zur Erstellung eines Testkatalogs geleistet, den ein automatisiertes Fahrsystem im Rahmen eines Gesamtvalidierungs- und -verifizierungsprozesses bestehen muss. Die Ergebnisse einer exemplarischen Umsetzung der Methode sind im Folgenden dargestellt.

3.1.1.4.9 Methode

1. Erkennung der Exposition von Szenario-Merkmalen wie Basis-Manöver oder Infrastrukturelementen.
2. Bewertung der potenziellen Schadensschwere entsprechend der Szenario-Merkmale basierend auf z.B. der GIDAS-Unfalldatenbank.
3. Anteilige Auswahl von risikobasierten Fällen aus der Schadensschwere- und Auftrittshäufigkeitsverteilung als Grundlage für funktionale Szenarien.
4. Umwandlung in funktionale Szenarien und Testfälle.
5. Katalogisierung von risikobehafteten Szenarien zur Abdeckung maximaler Risiken in einer begrenzten Anzahl von Tests.

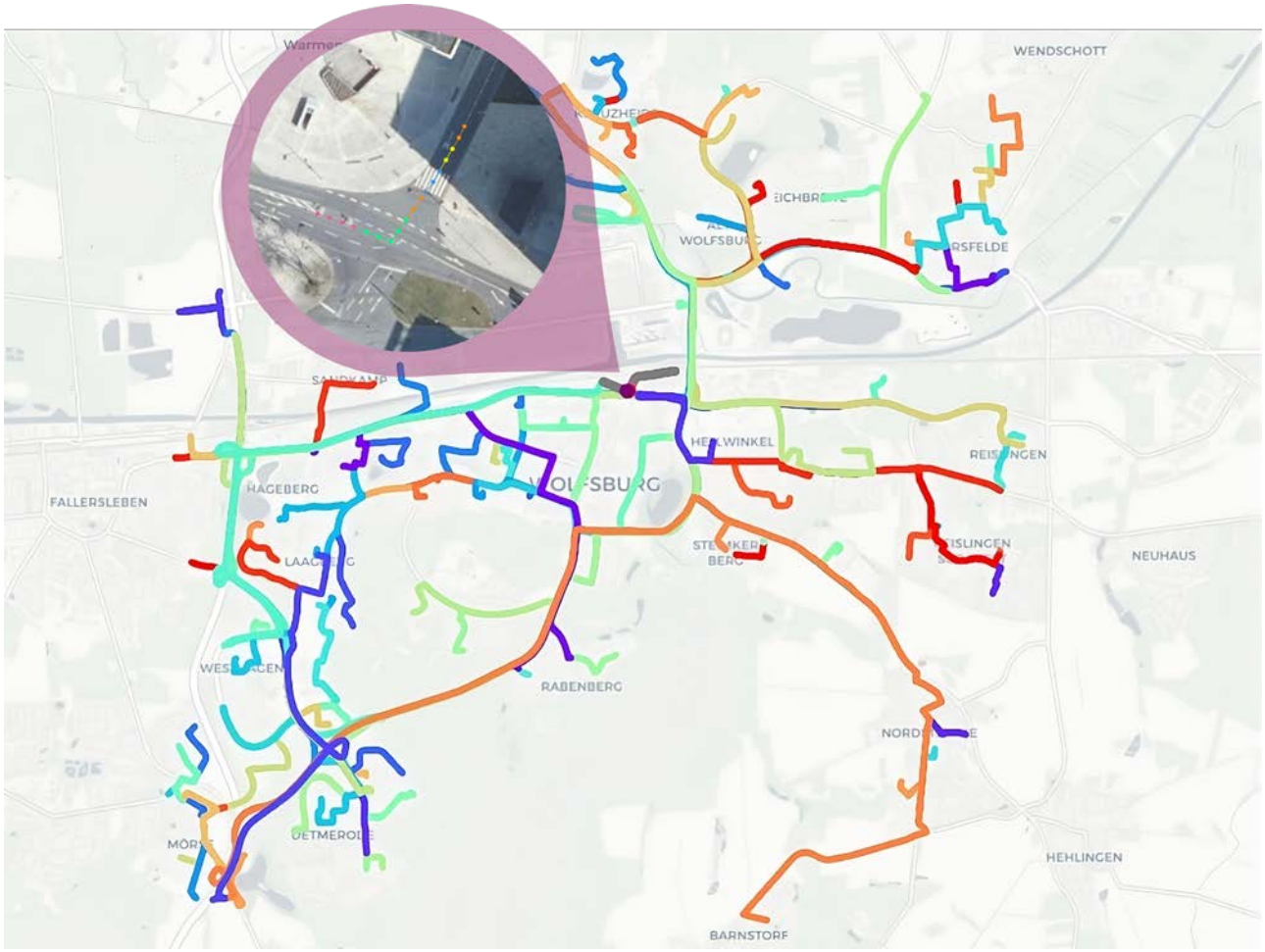


Abbildung 90: 100 Routen im Geofence von Wolfsburg generiert. (©Volkswagen AG)

3.1.1.4.10 Ergebnisse

- 100 beispielhafte Routen in OpenStreetMap generiert
- 38.417 erfasste Merkmale, verbunden mit 624.722 Kritikalitätsphänomenen
- 8.365 extrahierte Szenarien, nach Risikobewertung sortiert
- Verallgemeinerung erkannter Szenarien zu funktionalen Szenarien über die erkannten Merkmale

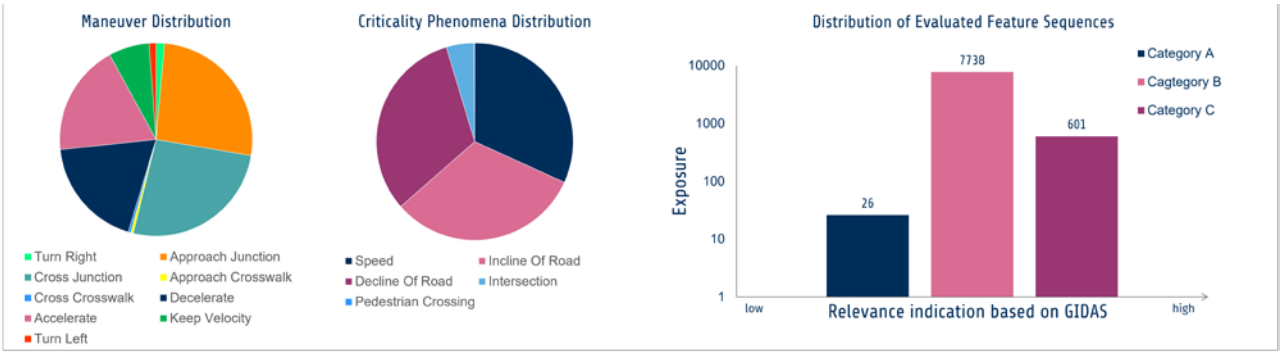


Abbildung 91: Links: Verteilung der erkannten Features. Mitte: Verteilung der erkannten Kritikalitätsphänomene. Rechts: Drei beispielhafte Feature Sequenzen, sortiert nach den Auftrittshäufigkeiten in den generierten Routen (©Volkswagen AG).

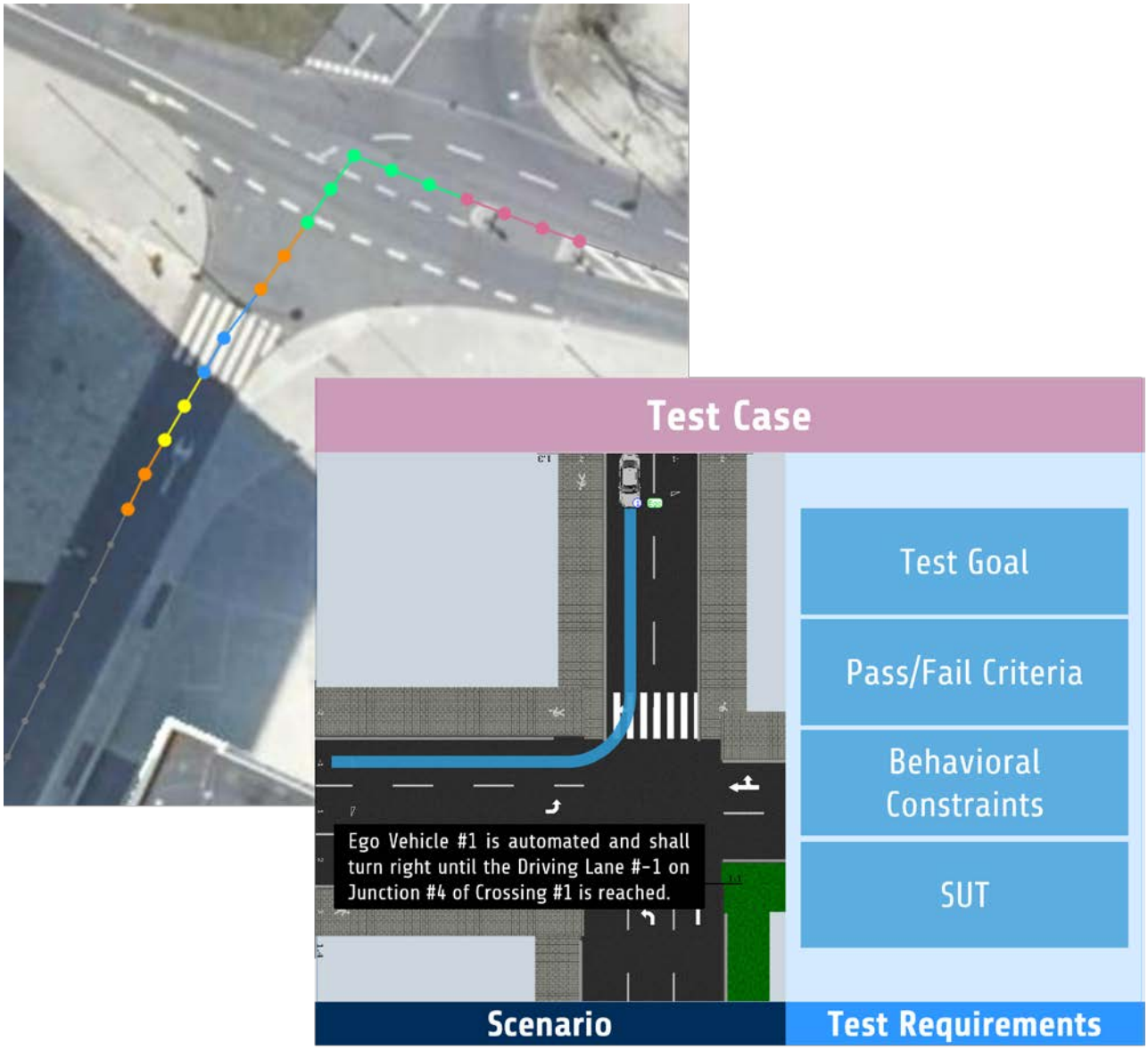


Abbildung 92: Links: Beispielhafte Feature Sequenz entnommen aus den generierten Routen. Rechts: Kombination der Ergebnisse in einen beispielhaften Testfall gebaut in stiEF [63] angereichert mit Testanforderungen (©Volkswagen AG).

3.1.1.4.11 Fazit

Die Methode ermöglicht die Erstellung eines endlichen Testfall-Katalogs von risikobehafteten funktionalen Szenarien, indem sie Szenariomerkmale in Eingangsdaten erkennt und diese mit Kritikalitätsphänomenen kombiniert. Das Resultat der Kombination ist eine risikobasierte Verteilung von katalogisierten Testfällen. Abhängig vom Anwendungsfall kann die Testtiefe mittels der Anzahl der getesteten Testfälle aus der risikobasierten Verteilung angepasst werden. Es ist zu beachten, dass der Typ und die risikobasierte Verteilung der Testfälle maßgeblich von den verfügbaren Merkmalen in den Eingangsdaten abhängen. Zudem ist der potenzielle Schaden eine Schätzung, und die Zuordnung zu den erkannten Merkmalen kann weiter detailliert werden. Die dargestellten Ergebnisse basieren auf einer beispielhaften Implementierung und sind daher nicht repräsentativ.

3.1.1.5 Szenarienabstraktion - Szenariobasiertes Testen

In der VVM Gesamtmethode spielen Szenarien eine entscheidende Rolle, wie dies bereits in Kapitel 3.1.1.2 dargestellt wurde. Durch die Verwendung von Szenariomodellen, die unterschiedliche Detaillierungsgrade (funktional, logisch, konkret) ermöglichen, werden Szenarien gleicher Kategorisierungen ergänzt um eine Szenariendatenbank, die ein statistisches Modell der ODD in Form von Parameterverteilungen und Relevanz von Szenarien liefert, von der Konzeptfindung des ADS über eine Domänenanalyse, zu der die Kritikalitätsanalyse gehört, einer Verhaltensspezifikation, der Definition von Architekturen bis hin zur Ableitung von Testfällen für die Verifikation und Validierung benutzt. (siehe Abbildung 97) Dieser Abschnitt behandelt die Aspekte im Rahmen des Testens.

3.1.1.5.1 Warum szenariobasierte Tests?

Ein entfernungsbasierter Ansatz, wie er in der Vergangenheit für Assistenzsysteme bis zum SAE-Level 2 durchgeführt wurde, erfordert beispielsweise für ein SAE-Level 3 Autobahnsystem, eine unangemessen lange Teststrecke von ca. $7*10^8$ km, um ein Signifikanzniveau von 5 % zu erreichen. Die szenario- oder ereignisbasierte Methodik “rafft” die Ereignisse. Er bietet gegenüber dem streckenbasierten Ansatz, bei dem die Testfallgenerierung quasi zufällig über die gefahrene Strecke verteilt ist, den Vorteil eines systematischen und strukturierten Vorgehens. Für automatisierte Fahrsysteme der SAE-Level 3 und höher hat PEGASUS das szenariobasierte Testen etabliert. Abbildung 93 zeigt eine Gegenüberstellung beider Vorgehensweisen.

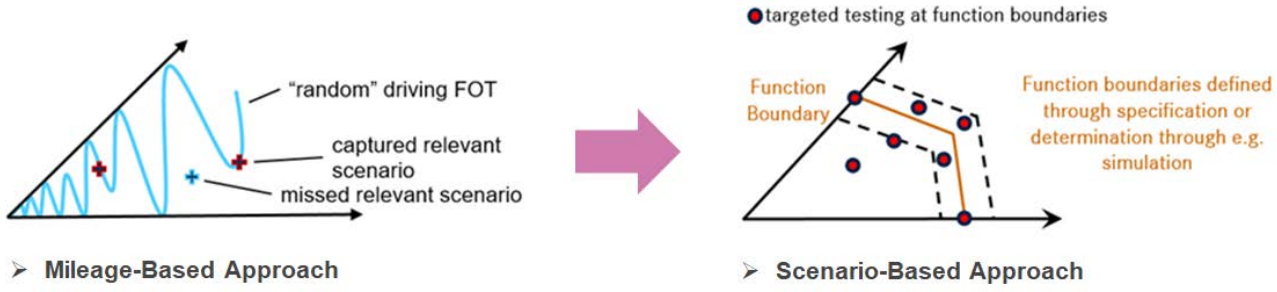


Abbildung 93: Gegenüberstellung “streckenorientiert” vs. “szenario- / ereignisorientiert”

Wo wird szenariobasiertes Testen im Rahmen der Gesamtmethodik für V&V eingesetzt?

Szenariobasiertes Testen wird im Rahmen der Bewertung und Risikoabschätzung (Abbildung 94) des ADS Release und der Validierung sowie im Rahmen der Verifikation eingesetzt.

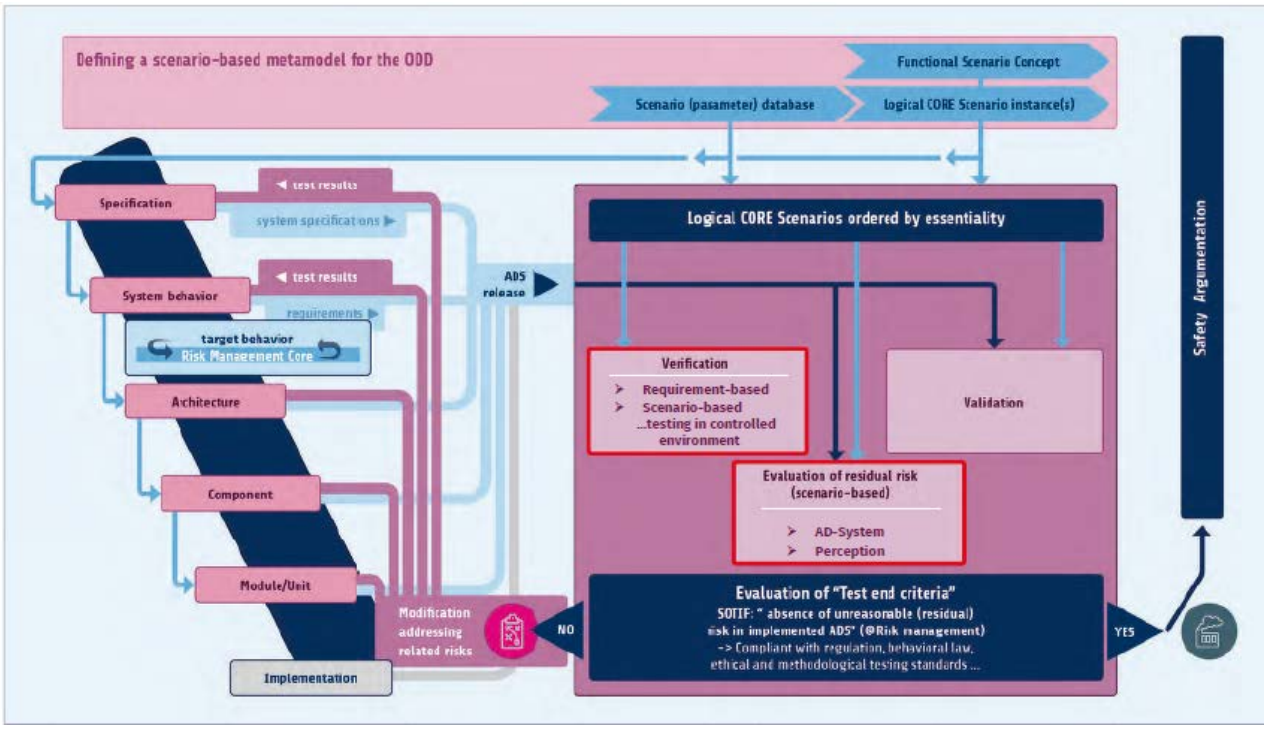


Abbildung 94: Scenario-based verification and Evaluation of the residual risk located in Development and safety insurance process.

Szenariobasierte Verifikation

Im Rahmen der Verifikation kann das szenariobasierte Testen zur Überprüfung von Testziele, wie z.B. der Überprüfung der korrekten Funktionalität und Performance, der Robustheit und der Erkennung von Systemgrenzen eingesetzt werden.

Die Methode der Szenarienraumanalyse wird auch zur Ableitung konkreter Testfälle auf dem Prüfgelände (Corner Cases oder Repräsentanten von Äquivalenzklassen) verwendet.

Um die Anzahl der Testfälle zu reduzieren, ist die Zerlegbarkeit der CORE-Szenarien (Szenarien, 6 Schichten, Parameter in jeder Schicht) sowie die Zerlegbarkeit der Funktionalitäten der ADS gegeben. Mit dem szenariobasierten Ansatz können auch ADS-Funktionalität in allen Funktionsschichten durch geeignete Parameterwahl getestet werden.

Das Verifikationskonzept ist Teil des V&V-Konzeptes. Es beschreibt den strategischen Ansatz beim Testen:

- Definition von unabhängigen Dekompositionsschichten und durchgängigen Schnittstellen,
- Definition von Pass/Fail-Kriterien für die Testfälle,
- Überprüfung der angemessenen Testabdeckung.

Die Testableitungsmethode „Analyse von CORE-Szenarien (Instanzen)“ und den darin enthaltenen Anwendungsfällen ist ein Werkzeug, mit dem Parameter strukturiert zerlegt und deren Einfluss analysiert werden können. Sie ist in Abbildung 95 dargestellt. Sie nutzt die Dekomposition der Menge der CORE Szenarien sowie für jedes einzelne CORE-Szenario in seinen instanziierten Beschreibungsebenen.

Sie wird für die Generierung von Testfällen in der Verifikation verwendet, um allgemeine Testziele wie "Funktionalität", "Performance" oder "Usability" nachzuweisen.

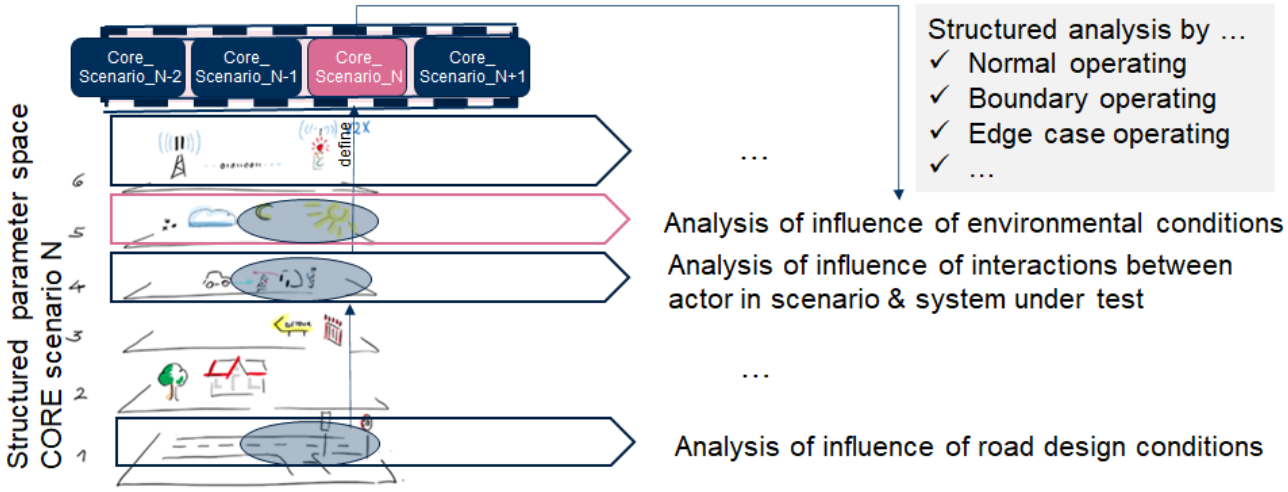


Abbildung 95: Scenario-based verification, decomposition of the scenario-based parameter space

Szenario-basierte Bewertung des Restrisikos

Im Rahmen dieses Prüfauftrages ist eine Bewertung des Restrisikos des (implementierten) ADS im szenariobasierten Metamodell der ODD vorzunehmen. Dies wiederum bedeutet, dass das Restrisiko für jedes CORE-Szenario in seinem (aktuellen) Parameterraum bestimmt werden muss. Dazu wird eine geeignete Bewertungsfunktion aus den TOP Safety Goals abgeleitet und in den Safety Goals und im V&V-Konzept definiert. Die Bewertungsfunktion kann z. B. das Risiko einer ADS-Auslösung in den CORE-Szenarien mit einer Kollision der Schweregrade S1, S2 und S3 sein.

Daraus ergibt sich dann das Ziel, konkrete kollisionsrelevante Parametersätze oder Parameterbereiche im Parameterraum für den Test zu identifizieren. Aufgrund der großen Anzahl der durchzuführenden Testfälle erfolgt die Zuordnung zu Testumgebungen durch ein ausgefeiltes Konzept - als Teil des V&V-Konzeptes - bestehend aus der Durchführung von Simulationen auf verschiedenen Testinstanzen, dem Nachweis der Gültigkeit der Ergebnisse der Simulationen auf dem Testgelände und der Felderprobung.

Die im Rahmen von VVM durchgeführten Arbeiten zeigen verschiedene Ansätze zur Bewältigung dieser Herausforderungen.

Szenario-basiertes Absichern

Im Rahmen des Verifikations- & Validierungskonzeptes wird für die Verifikation des ADS ein Testkonzept erstellt. Es definiert, was getestet wird (Testobjekte), wofür der Test den Nachweis der Konformität erbringen soll (Testziele), auf welchen Ebenen die verschiedenen Systemelemente getestet werden (Teststufen), enthält eine allgemeine Spezifikation des Testverfahrens zur Erreichung der Testziele (Teststrategien und die anzuwendenden Methoden zur Testfallableitung, KPI zur Testraumabdeckung und Testendekriterien), die verwendeten Testumgebungen (Testplattformen) und eine Testmatrix mit einer detaillierten Zuordnung der durchgeführten Tests zu den Systemanforderungen.

In Abbildung 96 wurden beispielhaft nachzuweisende Testziele auf der Systemebene aus den Klassen SOTIF, Systemperformanz, korrekte Funktion und Interface möglichen Methoden für die Ableitung von Testfallspezifikationen gegenübergestellt.

Methods for test case derivation / Test Goal (derived from Standards)	Requirement Analysis	Core Scenario analysis	Interface analysis
	test case derivation based on requirements & specifications depending on normal & border operating, & error conditions.	*test case derivation based on CORE scenario instances in varying parameters in layer (SUT & actors, weather, …)*	*test case derivation based on external or internal interface specifications (e.g. HW/SW interface).*
SOTIF (exemplary)			
S.1: Proof that the system properly detects that it is "inside" ODD, where it is designed to perform.	X	X	
S.2: Proof that the system properly detects that it is "outside" ODD, where it is designed **NOT** to perform.	X	X	
Performance (exemplary)			
Prof that test object provides its required functionality with regard to time & up to limits of its tolerance range	X	X	
correct functionality (exemplary)			
Proof that implemented functionality is as specified (correct processing inputs & outputs).	X	X	
correct interaction at the interfaces			
Proof of (external & internal) interfaces as specified.	X		X

Abbildung 96: beispielhafte Zuordnung von szenariobasierten Testzielen und Methoden zur Testfallableitung aus dem Testkonzept

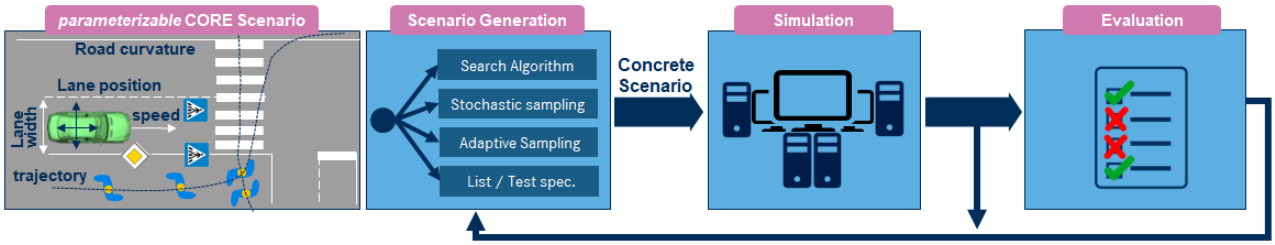
Szenarien und Testfälle

Requirements beschreiben das vom ADS erwartete Sollverhalten. Eine logische Szenario-Instanz definiert einen Parameterraum in dem die Überprüfung in konkreten Szenarien stattfinden kann. Diese Prüfungen verifizieren, ob das Testobjekt das geforderte Sollverhalten in der Menge aller Szenarien (Instanzen) tatsächlich hat, in denen das Requirement gelten soll. Diese Prüfaufgabe charakterisiert den Kern einer Testfall-Spezifikation (Abbildung 97). Mit Samplingverfahren werden aus dem Parameterraum eines Szenarios die Parameter ausgewählt, die tatsächlich geprüft werden und definiert die Güte der daraus resultierenden Abdeckung des Testraumes.

	Description	Planning
Initial test information	Test object (type), Test Goal, Test Levels & Plattform, Test Type, …, responsibilities	X / -
Initial methodical info	CORE scenarios & relevant sub parameter space for test case coverage, scanning method, …	x
Precondition	conditions which must be fulfilled before the test case is executed	x
Postcondition	conditions which are *"valid"* after the test case has been executed.	x
Test steps	Test steps contain actions and usually also expected results. **Init steps**: steps necessary to establish a state in which test steps of type "run" can be executed, i.e. this is a preparation or setup for the *"run step"* execution. **Run steps**: main test steps of a test case. These establish the core testing activities for which the results have to be evaluated. **Shutdown steps**: if the test object has to be put (back) into a certain state after test execution, shutdown steps can be executed.	x
Configuration parameter	Release level, parametrization of test object, (concrete) scenario parameter, …	X/-
Pass / Fail criteria	Criteria that describes the expected result for an executed test. The description has to be in a form in which the test results can be judged as either *"passed"* or *"failed"*.	x
Abortion criteria	Criteria that describes the cancellation criteria apply to performed test level.	x
prioritization	State the set of rules you wish to apply to assign priority to test cases.	x
Linked requirements	links from a test case to those *"requirements"* which shall be tested by the test case.	x

Abbildung 97: Beispielhaftes Format für eine detaillierte (technische) Testfall-Spezifikation

Die folgende Abbildung 98 zeigt unterschiedliche Methoden, wie aus Testfallspezifikationen mit unterschiedlichen Samplingverfahren konkrete Tests im Parameterraum abgeleitet werden können.



	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

Abbildung 98: Szenariobasiertes Testen - verschiedene Merkmale / Anwendungsbereiche

Eine wesentliche Herausforderung beim szenariobasierten Testen ist es konkrete Testfälle zu generieren. Dies kann auf unterschiedliche Arten von statten gehen. Einerseits können konkrete Szenarien mit Samplingmethoden, die auch durch geeignete Heuristiken ergänzt werden, in den Parameterräumen der CORE Szenarien bestimmt werden, andererseits kann die Szenario-Datenbank verwendet werden, um statistische Abhängigkeiten von Parametern oder Parameterklassen zu nutzen. Dies kann auf unterschiedliche Art und Weise umgesetzt werden:

- durch Nutzung von Verteilungen von Parametern und deren Korrelationen für Sampling-Verfahren oder
- durch geeignete Auswahl von konkreten Szenarien, die in der Szenario-Datenbank enthalten sind.

Dies führt unter anderem zu den folgenden Vorgehensweisen:

Methoden zur Reduktion bzw. Optimierung des Testaufwands

Die Restrisikoabschätzung wird als Optimierungsproblem formuliert und ein Lösungsvorschlag mittels nichtlinearer bzw. stochastischer Methoden vorgestellt.

Risikobasierte Auswahl konkreter (Test-)Szenarien für ein logisches Szenario

Die Idee ist, den Szenarienraum in Parameterteilräume (Szenarien) mit niedrigem, mittlerem und hohem Risiko zu clustern und daraus Stichproben zu ziehen (z.B. prozentual höherer Anteil von Testfällen aus dem Hochrisikocluster) um dann nur diese zu testen. Die Auswahl relevanter Szenarien, die repräsentativ für den gesamten Parameterraum sind, ist hier die Idee. Dadurch kann der Testaufwand deutlich reduziert werden.

Anforderungen an die Reduktion von Szenarien

Das Ziel der Szenarienauswahl besteht darin, relevante Szenarien auszuwählen, die den gesamten Parameterbereich so repräsentativ wie möglich abbilden. Dabei wird angenommen, dass es möglich ist, Szenarien zu identifizieren, die für andere Szenarien repräsentativ sind. Hierfür wird ein logisches Szenario mit verschiedenen Parametern als Ausgangspunkt genommen.

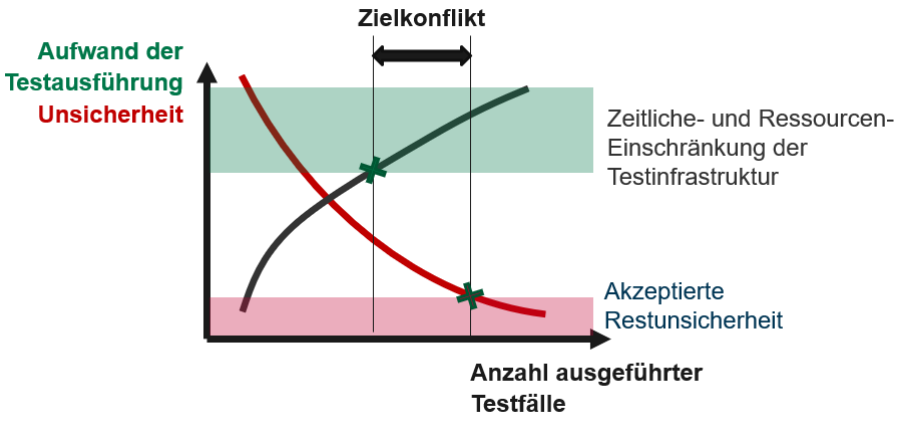


Abbildung 99: Zielkonflikt bei der Auswahl und Priorisierung von Testfällen

Bestehende Methoden werden aufgegriffen und auf die spezifischen Anforderungen übertragen, um zu einem Gesamtstatement zu gelangen. Das Ziel besteht darin, den erforderlichen Simulationsaufwand zu reduzieren. Durch die Auswahl repräsentativer Szenarien können Erkenntnisse gewonnen werden, die idealerweise auf unterschiedliche Systeme übertragbar sind. Dies ermöglicht eine effizientere Analyse und Bewertung von Systemen, da der Fokus auf besonders aussagekräftigen Szenarien liegt. Durch die Integration bestehender Methoden wird eine solide Grundlage für die Ableitung von Schlussfolgerungen geschaffen, wodurch der Gesamtnutzen des Simulations- bzw. Testaufwands maximiert wird.

Samplingverfahren können die Parametersätze für die konkreten zu prüfenden Szenarien algorithmisch aus mathematischen Räumen auswählen oder sie aus einer Szenariendatenbank auswählen, in der zu den logischen Szenarien in der Realität beobachtete Repräsentanten enthalten sind. Einen methodischen Zugang hierfür beschreibt der folgende Abschnitt.

Generierung konkreter Parameter aus logischen urbanen Fahrszenarien auf Basis hybrider Graphen

Für die vorgestellte Methode werden logische Szenario-Instanzen und ein Verfahren zum Samplen von realistischen Fahrszenarien daraus benötigt. Dazu wurde ein Vorgehen entwickelt, welches wissensbasierte Methoden mit datengetrieben Methoden kombiniert, um Parameterverteilungen logischer Szenarien zu schätzen und daraus realistische Fahrszenarien zu sampeln. Dabei werden hybride Graphen für die Modellierung der Parameter und deren kausalen Beziehungen und Abhängigkeiten benutzt. Die Beziehungen unter Parametern kann man in zwei Gruppen unterteilen:

- Deterministisch beschreibbare Relationen: Beziehungen zwischen Parametern, die eindeutig durch deterministische mathematische Gleichungen oder Ungleichungen dargestellt werden können.
- Probabilistische Relationen: Beziehungen, die den kausalen Einfluss eines Parameters auf einen anderen beschreiben, der mit vertretbarem Aufwand nicht deterministisch modelliert werden kann.

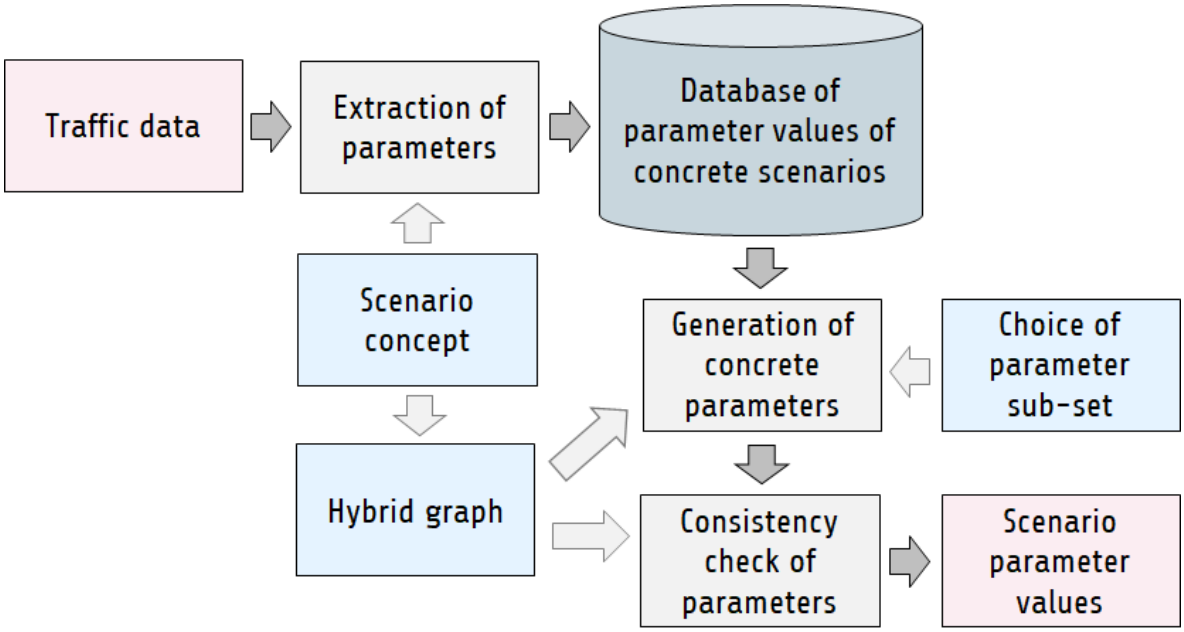


Abbildung 100: Prozess der Ableitung von Logischen Szenarien mit Parametern und deren Verteilung, sowie dem Sampling aus diesen.

Die Verwendung dieser beiden Arten von Beziehungen ermöglicht die Implementierung abhängiger Parameter und damit die Auswahl sinnvoller Teilgraphen für die Szenariengenerierung. Hierfür kann innerhalb von Einschränkungen eine Filterung relevanter Szenarien angewendet werden. Durch einen modularen Ansatz für die Herleitung von Parametern können verschiedene Einflüsse innerhalb eines Szenarios kombiniert werden, indem Graphen, die einzelne Konzepte bzw. deren Parameter beschreiben, zusammengeführt werden. Zur Generierung von Szenarien wird ein dreistufiger Ansatz verwendet. Dabei werden sowohl probabilistische Copulas für die Generierung kontinuierlicher Parametersätze als auch kausale Bayes'che Netze für die kausale Inferenz genutzt.

1. Initiale Generierung von Parameterwerten: Verwendung multivariater Copulas zur Ziehung von Samples kontinuierlicher Parametersätze.
2. Einschränkungsprüfung und -korrektur: Anpassung und Überprüfung der generierten Parameter gemäß den Einschränkungen des hybriden Graphen.
3. Berechnung der kausalen Wahrscheinlichkeit: Berechnung der Eintrittswahrscheinlichkeit basierend auf kausalen Kanten unter Verwendung von mit Bayes'schen Netzwerk modellierten bedingten Beziehungen.

Die untenstehende Grafik zeigt so einen Hybriden Graphen am Beispiel der Parameter der Basis-Szenarios “Merging Following Conflict”.

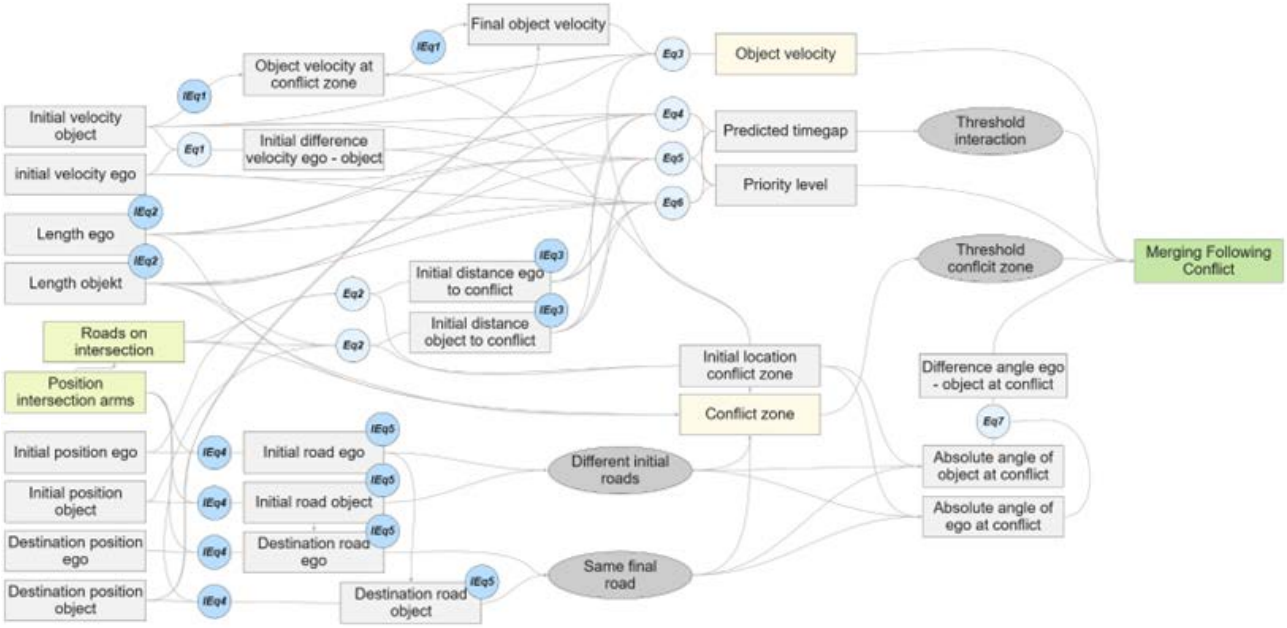


Abbildung 101: Beispiel des Hybriden Graphen der Parameter des logischen Szenarios “Merging Following Conflict”

3.1.1.5.2 Methoden zur Reduktion und Optimierung des Testaufwands beim szenariobasierten simulativen Testen der automatischen Funktionalität und Evaluierung des verbleibenden Restrisikos.

Innerhalb der VVM-Gesamtmethodik dient die Bewertung des Risikos, das von der ADS ausgeht, als wesentliche Kennzahl in der ODD, beispielsweise für die Bewertung des Verhaltens des Systems (funktionelle & verhaltensbezogene Sicherheitsanforderungen) als hinreichend sicher, sowie in der Verifikation & Validierung als Indikator innerhalb des Kriteriums "Testende". Das verbleibende Risiko stellt somit einen wichtigen Indikator dar, um zu überprüfen, ob ein wesentlicher Aspekt der Funktionalität gegeben ist.

Zu diesem Zweck wird eine entsprechende Bewertungsfunktion im Konzept der Verifikation und Validierung definiert. Beispielsweise kann die Bewertungsfunktion das Systemrisiko einer Kollision in einem CORE-Szenario in den Schweregraden S0, S1, S2, S3 bewerten.

Das abgeleitete Ziel ist dann z.B. die Identifizierung von kollisionsrelevanten Parametersets / -grenzen oder Bereichen im Parameterraum. Die Funktionalität ist nach Relevanz zu zerlegen.

Eine zentrale Testaufgabe ist die Bewertung des Restrisikos der ADS im szenariobasierten Metamodell der ODD. Dies umfasst die Bewertung des Restrisikos für jedes CORE-Szenario in seinem Parameterraum.

Die Core-Szenarien lassen sich in das Szenario, die Beschreibungsebene des Szenarios und die in der Ebene deklarierten Parameter zerlegen. Die Restrisikoabschätzung erfolgt somit für jedes CORE-Szenario einzeln und sukzessive. Auf Basis realer Messdaten und unter Verwendung der Szenario-(Parameter-)Datenbank werden die Wahrscheinlichkeitsverteilungen der deklarierten Parameter jeder Schicht der CORE-Szenario-Instanz sowie die Häufigkeit des Eintretens des jeweiligen Szenarios (Exposition) bestimmt.

Korrelationen zwischen den Parametern der Szenarien müssen in Betracht gezogen werden. Der gesamte Prozess muss so gestaltet werden, dass eine möglichst hohe Abdeckung aller kritischen

Bereiche des Parameterraums erreicht wird. Andernfalls besteht die Gefahr, dass wichtige Schwachstellen des Systems unentdeckt bleiben und die Risikobewertung verzerrt wird. Zu diesem Zweck kommt ein mehrstufiges Verfahren zum Einsatz, das über die gezielte Generierung neuer Szenariomerkmale, Optimierungsansätze und eine anschließende Clusteranalyse die wichtigsten kritischen Parameterbereiche identifiziert und für weitere statistische Analysen aufbereitet. Grundlage ist eine Formulierung als Optimierungsproblem mit Kritikalitätsmaß und Pass/Fail-Kriterien im Parameterraum. Eingesetzt wird das "search based testing".

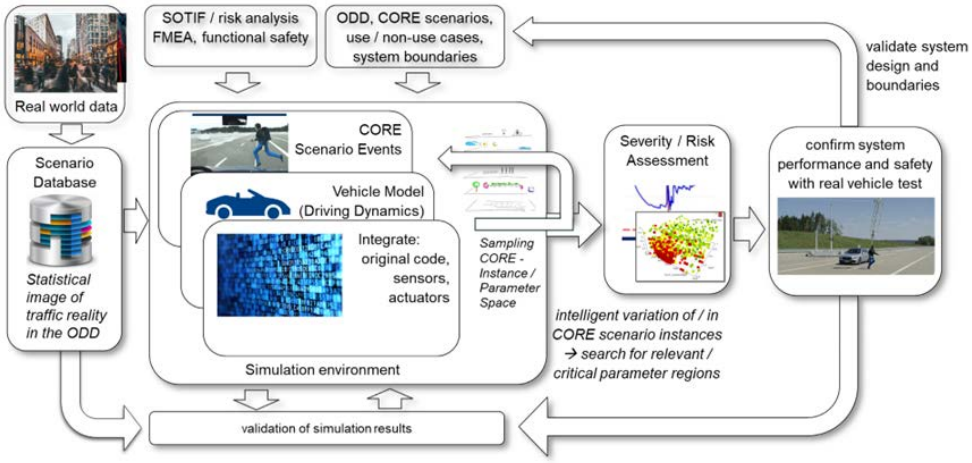


Abbildung 102: Simulation-based process; search-based testing

Parameterreduktion durch Sensitivitätsanalyse:

Durch den Einsatz von Methoden der Sensitivitätsanalyse (z. B. DoE & Regression) werden die erklärten Parameter identifiziert, die den größten Beitrag zu einer möglichen Verbesserung der Zielfunktion leisten. Hierdurch wird eine effektive Zerlegung und Schätzung des Stichprobenumfangs ermöglicht.

Der Parameterraum der CORE-Szenario-Instanz wird (für die identifizierten sensitiven Parameter) mit einem intelligenten Algorithmus durchsucht, um die Eintrittswahrscheinlichkeit einer kritischen Situation oder einer Kollision zu bestimmen. Als Nebenprodukt erhält man eine Charakterisierung des Parameterraums in Kategorien für den Schweregrad: Identifikation von Teilräumen mit sicherheitstechnischen Mängeln, z. B. Kollisionen mit hohem oder mittlerem Schweregrad, Identifikation von Grenzwerten für sicherheitsrelevante Schäden, Abschätzung von Verletzungswahrscheinlichkeiten.

Samplingverfahren können nichtlineare Optimierungsverfahren sein, wie evolutionäre Algorithmen, Partikelschwarm, simuliertes Annealing, lokale Optimierungsverfahren, etc.. Adaptive Stichprobenverfahren können an den Rändern von Sicherheitsverletzungen (Grenzen zwischen Kritikalitätsklassen) eingesetzt werden.

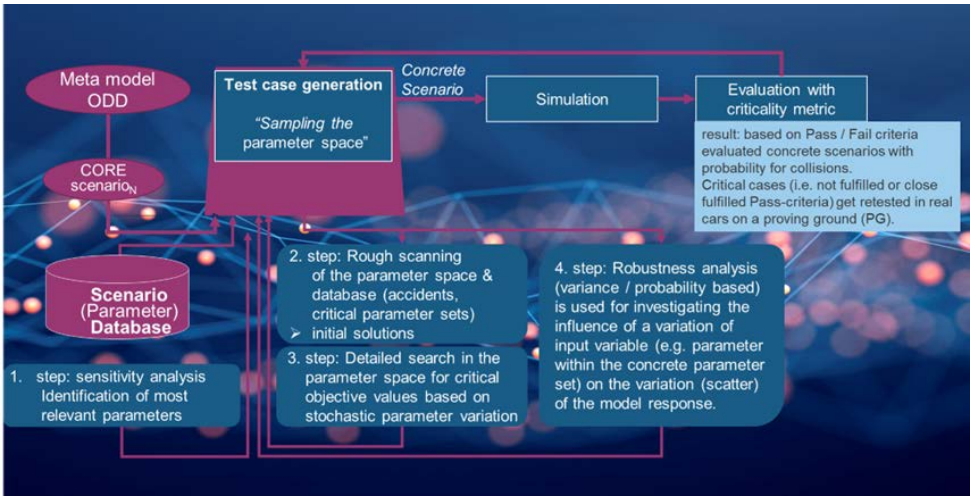
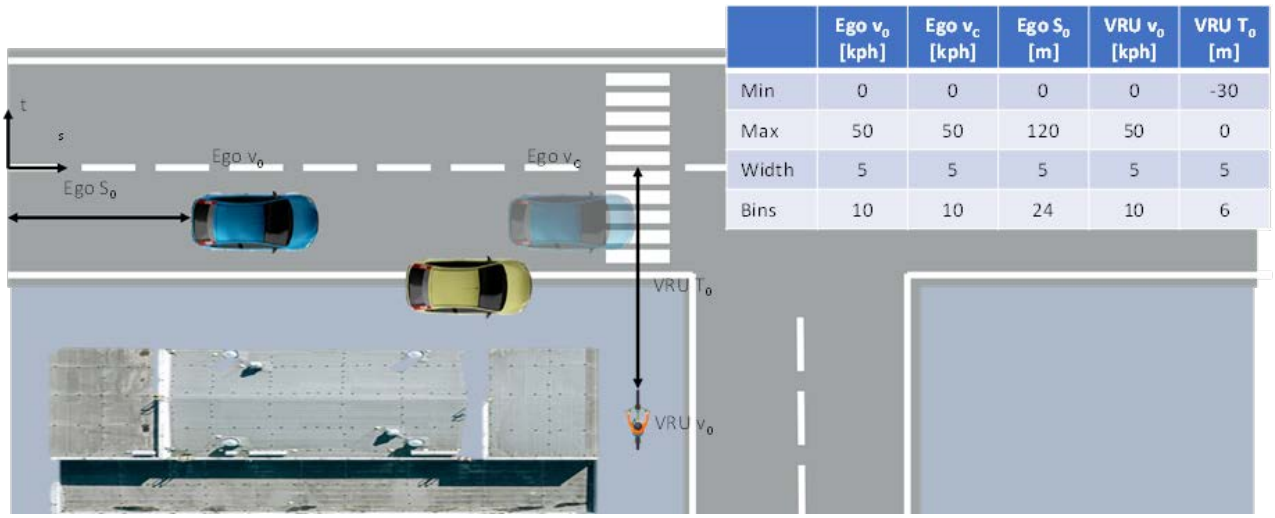


Abbildung 103: Simulation-based risk assessment

3.1.1.5.4 Risiko-basierte Auswahl von konkreten Testszenarien für ein CORE Szenario

Die Ableitung konkreter (Test-)Szenarien für ein gegebenes logisches Szenario ist einer der Schlüsselfaktoren für einen effektiven Testprozess. Der durch ein logisches Szenario definierte Szenarioraum enthält eine große Anzahl möglicher konkreter Szenarien, von denen einige "interessanter" sein können als andere (basierend auf ihrem individuellen Risiko). Die Idee der risikobasierten Auswahl von (Test-)Szenarien besteht darin, den Szenarienraum in Szenarien mit niedrigem, mittlerem oder hohem Risiko (oder auch mehr) zu clustern und für diese clusterindividuelle Samplingstrategien anzuwenden (z.B. prozentual höherer Anteil von Testfällen aus dem Hochrisikocluster). Dabei sollten auch alltägliche Fahrszenarien berücksichtigt werden.



	Ego v_0 [kph]	Ego v_c [kph]	Ego S_0 [m]	VRU v_0 [kph]	VRU T_0 [m]
Min	0	0	0	0	-30
Max	50	50	120	50	0
Width	5	5	5	5	5
Bins	10	10	24	10	6

Abbildung 104: Logisches Szenario mit fünf Szenarioparametern, deren Grenzwerten und Abstufungen

Abbildung 104 zeigt ein beispielhaftes logisches Szenario mit fünf Szenarioparametern und den dazugehörigen Bereichen. In diesem Beispiel können 144.000 verschiedene konkrete Szenarien erstellt werden, von denen jedes einzelne mehr oder weniger interessant für den Test sein kann. Nach Anwendung einiger Einschränkungen (z. B. "Ego und VRU kommen gleichzeitig am Zebrastreifen an", "Abstand zwischen Ego-Start und Zebrastreifen lang genug für Abbremsung") bleiben 5.122 konkrete Szenarien übrig. Für diese zeigt Abbildung 105 eine automatisierte

Risikobewertung nach gängigen Risikobewertungsparametern wie Szenariowahrscheinlichkeit und potenziellem Schweregrad.

S1 (v_{impact} < 15 kph)			S2 (15 kph ≤ v_{impact} < 43 kph)			S3 (v_{impact} ≥ 43 kph)		
920 (18%)			3633 (71%)			469 (9%)		
E1	E2	E3	E1	E2	E3	E1	E2	E3
616 (67%)	254 (28%)	50 (5%)	2390 (66%)	824 (23%)	419 (11%)	469 (100%)	0 (0%)	0 (0%)
gering	gering	mittel	gering	mittel	hoch	mittel	hoch	hoch

Geringes Risiko	3260 (64%)
Mittleres Risiko	1343 (26%)
Hohes Risiko	419 (8%)

- > 50% treten selten auf und beinhalten zusätzlich ein geringes Risiko
- Test-Fokusierung auf Parameterkombinationen mit ...
  - a) Hohem Risiko ("Edge case")
  - b) Hoher Auftretenswahrscheinlichkeit ("Alltagssituationen")

Abbildung 105: Beispielhafte Risikobewertung des FUC2.3 für die berücksichtigten Parameter, ihre Diskretisierung und sich ergebende Kombinationen

Für die Abschätzung der Auftretenswahrscheinlichkeit wurde ein realer Fahrdatensatz von ca. 25.000 km Stadtfahrt verwendet. Der Schweregrad wurde auf der Grundlage der potenziellen Aufprallgeschwindigkeit bewertet, wobei davon ausgegangen wurde, dass das Fahrzeug unmittelbar mit voller Verzögerung bremst, sobald die VRU sichtbar wird. Anhand von drei Auftretenswahrscheinlichkeits- und Schweregradklassen werden alle Szenarien entweder einem niedrigen, mittleren oder hohen Risikocluster zugeordnet.

Ergebnisse und Schlussfolgerung

Aus der Risikobewertung geht hervor, dass mehr als 50% der konkreten Szenarien ein geringes Risiko aufweisen und unter den getroffenen Annahmen in der Realität nur selten auftreten (Abbildung 105 S1E1 und S2E1). Ein hoher Testaufwand für dieses Cluster erscheint daher nicht sinnvoll. Stattdessen könnte es effizienter sein, sich auf Szenarien mit hohem Risiko (Abbildung 105 S2E3, S3E2, S3E3) und hoher Exposition (SxE3) zu konzentrieren, indem für diese Cluster geeignete Samplingstrategien gewählt werden.

Der vorgestellte Ansatz bietet die folgenden Hauptvorteile:

1. Er ermöglicht es, den Testaufwand auf interessante Szenario-Cluster innerhalb des Szenarienraums zu konzentrieren.
2. Er knüpft direkt an die Bewertung der positiven Risikobilanz (PRB) als ein Gesamtkriterium an.
3. Unter den getroffenen Annahmen erlaubt es eine Argumentation für ausreichende Vollständigkeit.
4. Sie orientiert sich an der ISO 34502 [48] zu Testszenarien für automatisierte Fahrsysteme.

3.1.1.6 Kritikalitätsanalyse

3.1.1.6.1 Der Prozess der Kritikalitätsanalyse

Die Kritikalitätsanalyse in VVMethoden ist eine Methode zur Analyse des offenen Kontexts der Operational Domain (OD) hinsichtlich der Entstehung von Kritikalität. Der grundlegende Ansatz besteht darin diesen offenen Kontext, welcher aus unendlich vielen Situationen und Szenarien

besteht, auf eine endliche und übersichtliche Menge von sicherheits-relevanten Artefakten abzubilden. Diese Artefakte sind unterteilt in 1) Kritikalitätsphänomene, 2) deren Wirkzusammenhänge sowie 3) abstrakte Szenarien welche die Vorigen instanziieren [57]. Diese grundlegende Idee ist schematisch in Abbildung 106 dargestellt.

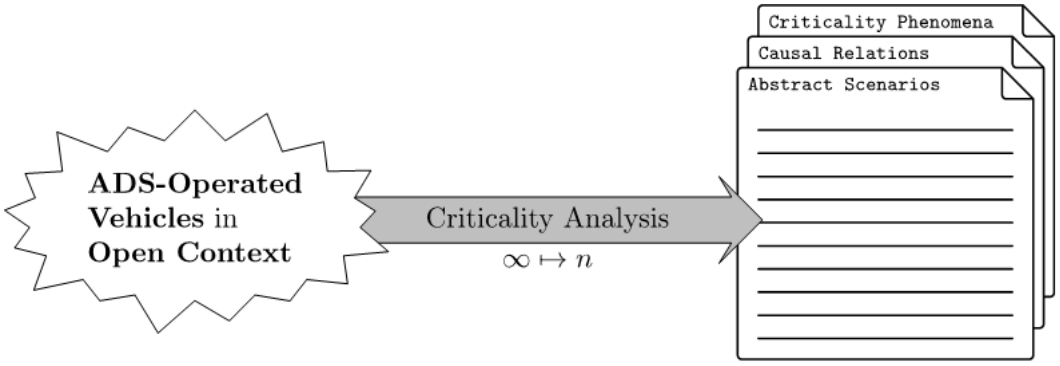


Abbildung 106: Grundlegende Idee der Kritikalitätsanalyse [57]

Im Projekt VVMethoden verortet sich die Kritikalitätsanalyse im operationellen Konzept (‘operational concept’) des VVM Absicherungrahmen ('assurance framework'). Die aus der Kritikalitätsanalyse resultierenden Artefakte werden dort insbesondere zur Herleitung des Sollverhaltens des zu entwickelnden automatisierten Fahrsystems (AF) eingesetzt. Auch eine Anwendung im Bereich der Testplanung ist möglich, bspw. zur Ableitung von Testszenarien.

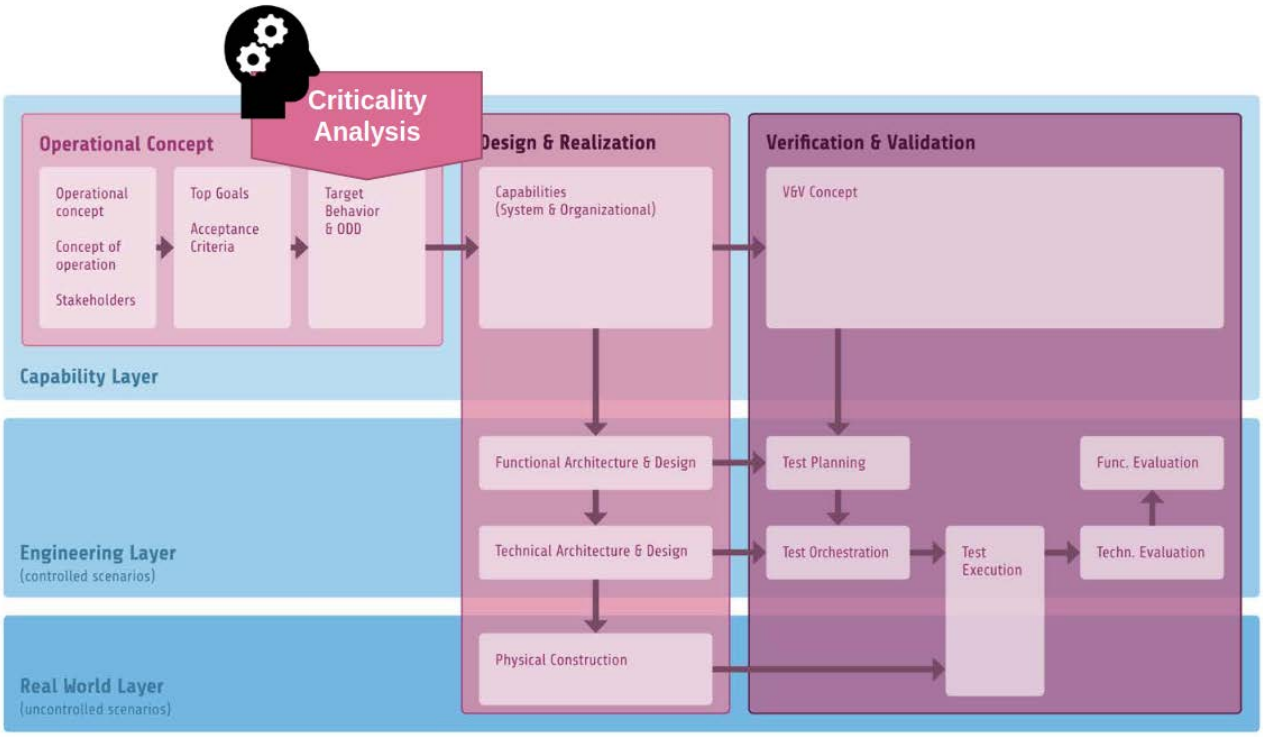


Abbildung 107: Verortung der Kritikalitätsanalyse im VVM ‘Assurance Framework’.

Die folgende Definition wurde in VVMethoden unter den Partnern diskutiert, abgestimmt und veröffentlicht (vgl. [57] Definition 1):

Definition: Die **Kritikalität** (einer Verkehrssituation) ist das kombinierte Risiko der involvierten Akteure wenn die Situation fortgesetzt wird.

Diese qualitative Definition legt den Grundstein für die Beantwortung der folgenden Fragen durch eine Kritikalitätsanalyse für eine Klasse von AF:

- Wann tritt Kritikalität in der OD auf?
- Was versucht diese erhöhte Kritikalität?
- Wie kann Kritikalität quantifiziert werden?
- Welche sind die kritischen Szenarien?

Um zu verstehen wie die Kritikalitätsanalyse diese Fragestellungen behandelt, ist zunächst ein tieferes Verständnis des Prozesses und der resultieren Artefakte notwendig.

3.1.1.6.1.1 Gesamtprozess und Artefakte der Kritikalitätsanalyse

Der detaillierte Gesamtprozess ist durch Abb. 3 gegeben [64], siehe auch die Quellen [57] [65] [66] für frühere Versionen der Grafik. Die Kritikalitätsanalyse teilt sich in drei Teilgebiete: den Methoden-Zweig, den Informations-Zweig und den Szenarien-Zweig. Bevor die Zweige verstanden werden können, werden die Artefakte der Kritikalitätsanalyse eingeführt:

- *Kritikalitätsphänomene* (Criticality Phenomena, CP): Einflussfaktoren welche mit erhöhter Kritikalität assoziiert sind (Statistische Assoziation).
- *Wirkzusammenhänge* (Causal Relations, CR): Erstellen und Validieren von graphischen Modellen, welche erklären wie CP zu erhöhter Kritikalität führen (Kausalität).
- *Abstrakte Szenarien*: basierend auf CP und CR; Verbindung zur Szenario-basierten Entwicklung, zur Verifikation und Validierung von AF.

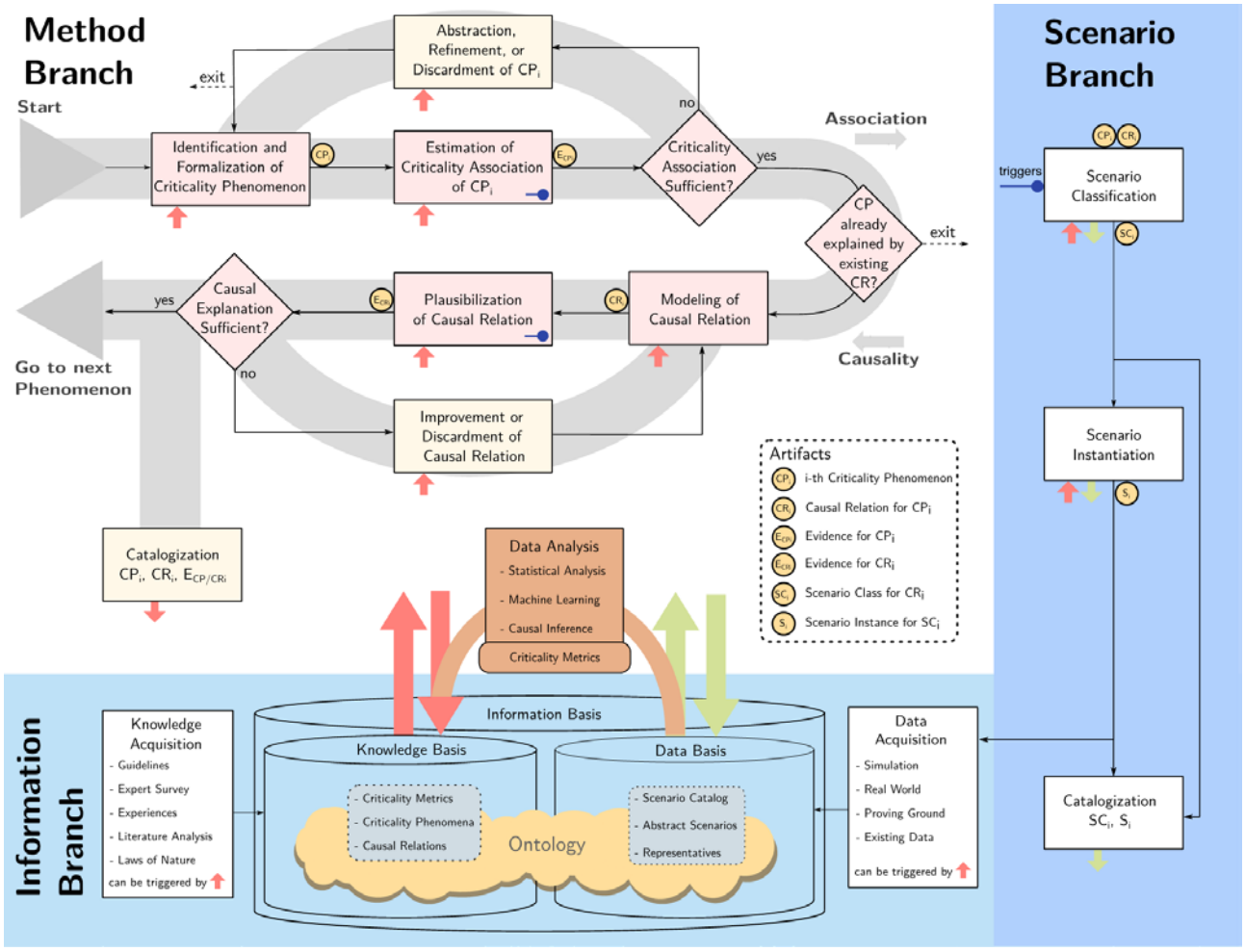


Abbildung 108: Übersicht zur Methodik der Kritikalitätsanalyse, strukturiert in die Teilgebiete Methoden-Zweig, Informations-Zweig und Szenarien-Zweig [64].

Der Methoden-Zweig ist der führende Zweig. Hier werden CP identifiziert, formalisiert und auf assoziative Relevanz geprüft. Anschließend werden die CR der CP modelliert und validiert. Dazu steht der Methoden-Zweig im stetigen Austausch mit dem Informations-Zweig, welcher Wissen und Daten organisiert und bereitstellt. Der Szenarien-Zweig wird vom Methoden-Zweig aufgerufen und verarbeitet die Artefakte CP und CR zu Szenarien(-klassen) welche im weiteren Entwicklungs- und Absicherungsprozess genutzt werden können.

3.1.1.6.1.2 Werkzeuge der Kritikalitätsanalyse

Zur Durchführung einer Kritikalitätsanalyse werden verschiedenste Werkzeuge eingesetzt:

- Ontologien zur formalen Darstellung der OD im Informationszweig und zu assoziative Analysen im Methoden-Zweig [67].
- Kritikalitätsmetriken zur Quantifizierung von Aspekten der Kritikalität [65].
- Verschiedene Methoden der Datenanalyse, u.a. Machinelles Lernen und Kausale Inferenz [68] [66].
- Simulationssysteme und -Modelle [69] [70].

3.1.1.6.2 Die Teilgebiete der Kritikalitätsanalyse

Wir beschreiben nun in Kurzfassung die verschiedenen Zweige der Kritikalitätsanalyse. Für eine ausgiebigere Beschreibung verweisen wir auf [57] Abschnitt 5 sowie [64] Abschnitte 3-5**.**

3.1.1.6.2.1 Der Methoden-Zweig

Der Methoden-Zweig der Kritikalitätsanalyse beschäftigt sich hauptsächlich mit den folgenden Fragen (vgl. Abbildung 109):

- Wie identifiziert und formalisiert man CP in der OD?
- Wie überführt man diese Assoziationen (also CP) zu plausiblen Kausalitäten (also CR)?

Der entsprechende Prozess wird durch Abbildung 109 schematisch dargestellt.

Die Kritikalitätsanalyse unterliegt hierbei zwei grundlegenden Annahmen:

1. Die Menge der relevanten CP ist endlich und überschaubar.
2. Relevante CP hinterlassen Spuren in einer wachsenden Datenbasis.

Während Annahme 1. die Endlichkeit der Artefakte der Kritikalitätsanalyse impliziert, impliziert Annahme 2. dass nach hinreichend vielen Iterationen eine Saturierung bzgl. dieser Artefakte auftritt.

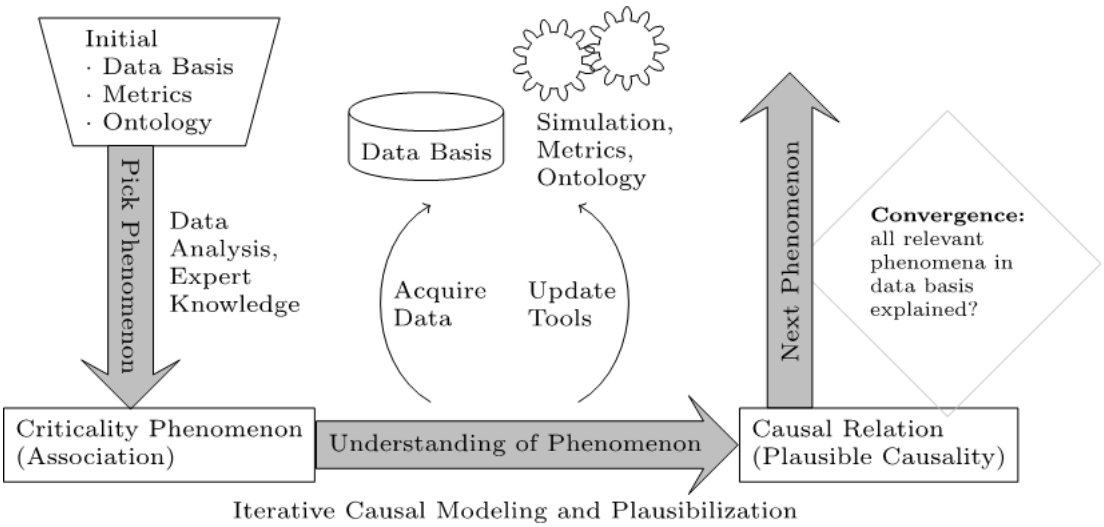


Abbildung 109: Der Methoden-Zweig - von Assoziation zu Kausalität [57].

Somit lässt sich der Methoden-Zweig somit in einen assoziativen und einen kausalen Teil gliedern:

3.1.1.6.2.1.1 Assoziativer Teil des Methoden-Zweigs

Der Methoden-Zweig beginnt mit der Identifikation von CP in der initialen Wissens- und Datenbasis. Die Generation von Hypothesen zu Kritikalitätsphänomenen basierend auf vorhandenem Wissen kann zunächst auf der Ebene von natürlicher Sprache stattfinden. Um jedoch Kritikalitätsphänomene in Daten, bspw. in einer Unfalldatenbank [66] oder in Drohnendaten [67], erkennen zu können, ist eine Formalisierung der CP sowie von messbarer Kritikalität notwendig. Um Uneindeutigkeiten zu vermeiden, können Kritikalitätsphänomene mit Hilfe einer

Ontologie formalisiert werden. In VVMethoden wurde hierfür „Automotive Urban Traffic Ontology“ (A.U.T.O.) aufgebaut und verwendet (siehe Informations-Zweig).

Für die Formalisierung (und damit auch Quantifizierung) von Kritikalität werden klassischerweise Kritikalitätsmetriken eingesetzt. Kritikalitätsmetriken sind mathematische Funktionen welche darauf abzielen gewisse Aspekte (z.B. Zeit oder Raum) von Kritikalität in einer Situation oder einem Szenario zu quantifizieren [65].

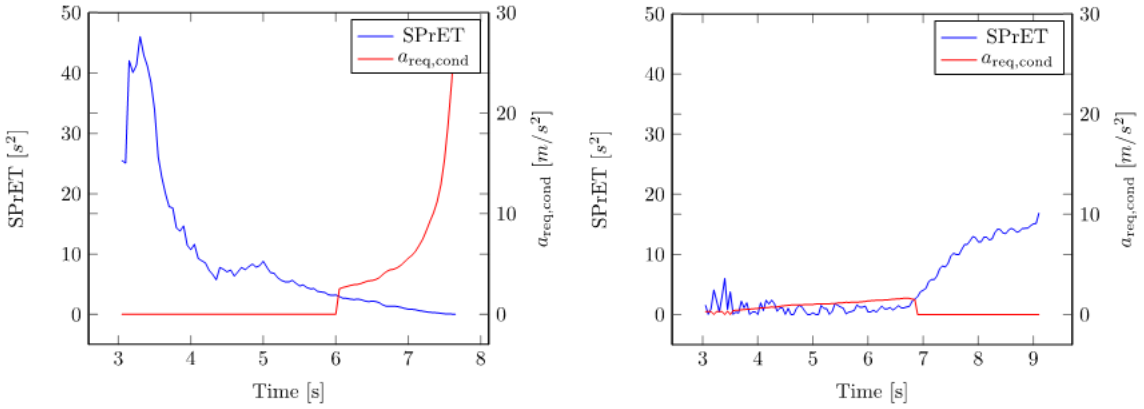


Abbildung 110: Zeitlicher Verlauf zweier Kritikalitätsmetriken (Conditional Required Acceleration (in rot) und Scaled Predictive Encroachment Time (in blau)) in einem kritischen Verdeckungsszenario (links) sowie einem unkritischen Szenario ohne Verdeckung. (© Neurohr et al. [57])

Die Formalisierung der CP gepaart mit via Kritikalitätsmetriken quantifizierter Kritikalität ermöglicht die iterative Abstraktion bzw. Konkretisierung der CP basierend auf der Stärke der Assoziationen in verschiedenen Datenquellen (siehe [67] [66].

3.1.1.6.2.1.2 Kausaler Teil des Methoden-Zweigs

Im Mittelpunkt des kausalen Teils des Methoden-Zweigs steht die Modellierung und Analyse von Wirkzusammenhängen (*causal relations*, CR) der Kritikalitätsphänomene (*criticality phenomena*, CP).

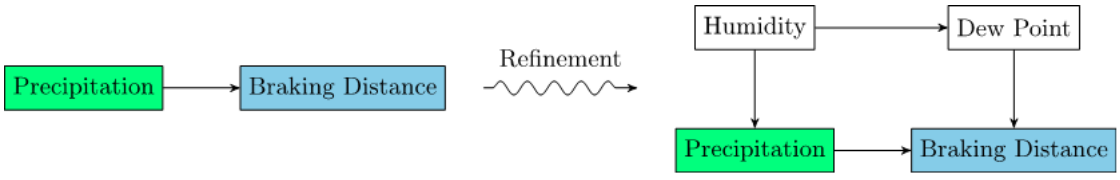


Abbildung 111: Konkretisierungsschritt in der Modellierung von Wirkzusammenhängen. (© Koopmann et al. [68])

Hierbei soll ein präzises Verständnis der zugrundeliegenden Beziehungen zwischen Ursache und Wirkung, die für das Entstehen von Kritikalität ausschlaggebend sind, erarbeitet werden. Dazu muss eine klare Abgrenzung zwischen reinen Assoziationen (zwei Artefakte treten oft zusammen auf) und plausiblen Kausalitäten (ein Artefakt verursacht ein weiteres Artefakt) stattfinden, um die Ursachen und Wirkungen klar voneinander trennen zu können. Der hierbei relevante Unterscheidungspunkt sind sogenannte Störfaktoren (Confounder), die sowohl die Ursache als auch die Wirkung beeinflussen und somit die wahre Beziehung von Ursache und Wirkung in Beobachtungsdaten verfälschen können (siehe Abbildung 112).

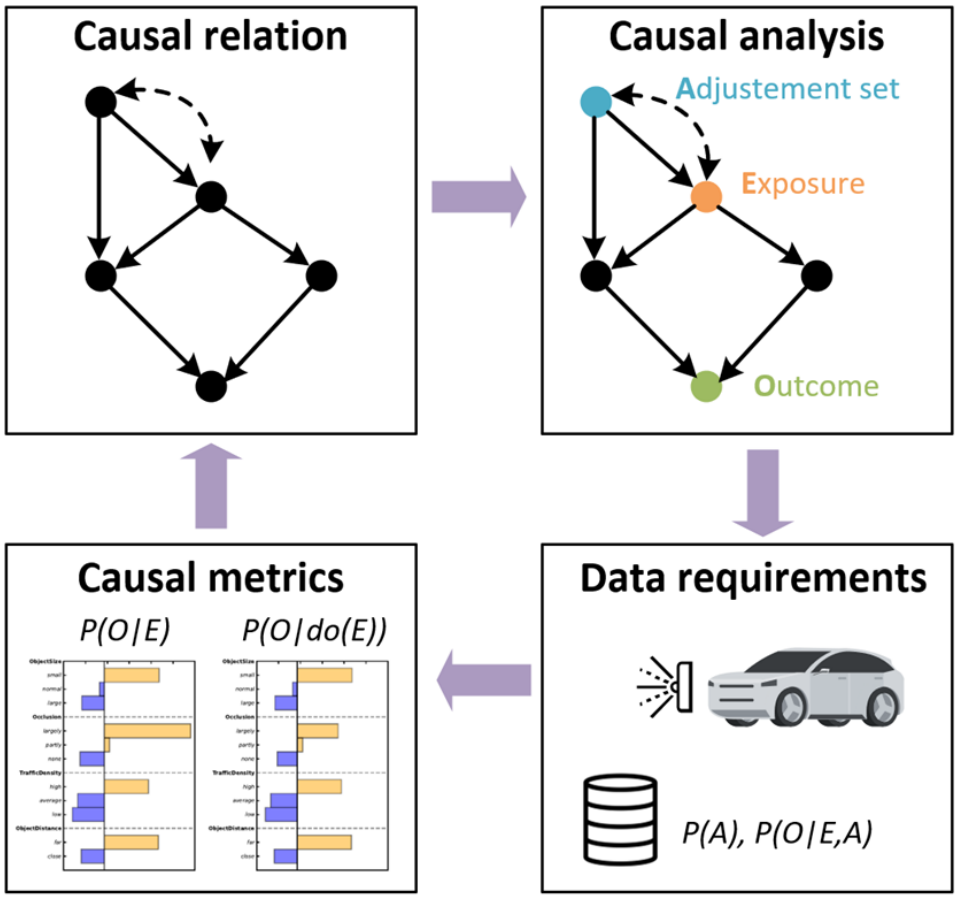


Abbildung 112: Workflow zur Modellierung und Analyse von Wirkzusammenhängen (© Robert Bosch GmbH)

Im Rahmen dieser Überlegungen wurden hierzu verschiedene Kausalitätsbegriffe betrachtet und anschließend insbesondere der Kausalitätsbegriff nach Judea Pearl näher untersucht. In dieser Theorie wird basierend auf einem Kausalgraphen argumentiert, welcher die kausalen Annahmen als Kanten im Graphen darstellt und somit zu einem verbesserten Verständnis und einer strukturierten Darstellung der zugrundeliegenden Kausalitäten führt. Hierbei wurden im Projekt insbesondere expertengetriebene Prozesse definiert und evaluiert, um die Kausalgraphen herleiten zu können. Anschließend wurden die aufgestellten Kausalgraphen mit Simulationsdaten angereichert, um eine Vielzahl untersuchter quantitativer Kausalitätsindikatoren (siehe z.B. [65] Abschnitt 3.3), zu evaluieren. Die daraus gewonnenen Erkenntnisse konnten in einer Rückkopplungsschleife zur weiteren Verfeinerung der Kausalgraphen durch Experten herangezogen werden.

Durch die Anwendung dieser Methode können basierend auf einer Menge von CP, Expertenwissen und Beobachtungsdaten, Anforderungen an die Datenerhebung, validierte CR und quantifizierte kausale Effekte der CP abgeleitet werden.

Für komplexe automatisierte Fahrfunktionen können oft keine deterministischen Modelle bestimmt werden. Die Methoden der kausalen Inferenz und Modellierung ermöglichen es jedoch, die Ursache-Wirkung-Beziehungen rein aus Beobachtungsdaten zu berechnen. Hierbei kann die kausale Modellierung sowohl auf der eher makroskopischen Ebene des Gesamtfahrzeugs als auch auf der Ebene der detaillierten Analyse einzelner Sensoren des Perzeptionssystems angewendet werden und jeweils wertvolle Beiträge leisten.

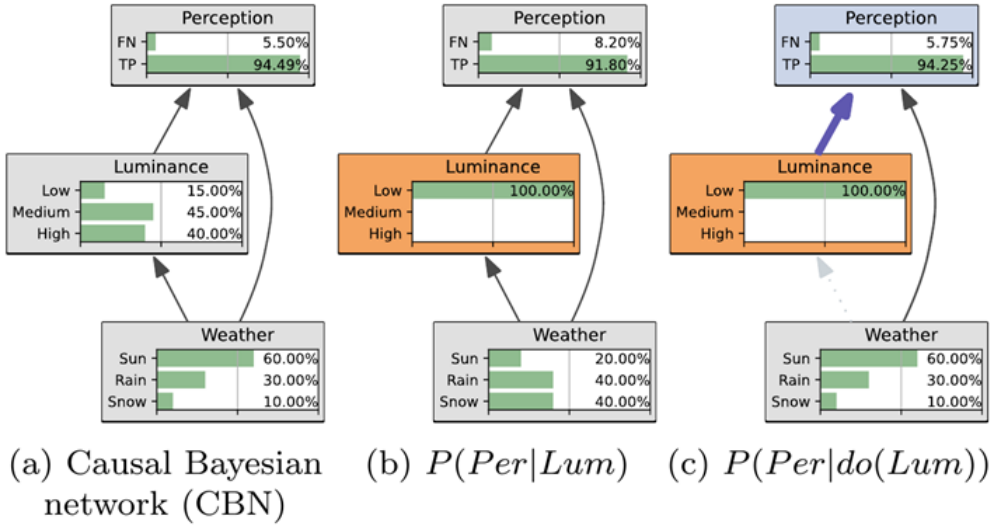


Abbildung 113: Effekt eines Störfaktors unter Nutzung reiner Beobachtungsdaten mit bedingten Wahrscheinlichkeiten und einer Herangehensweise über Interventionen der Kausaltheorie

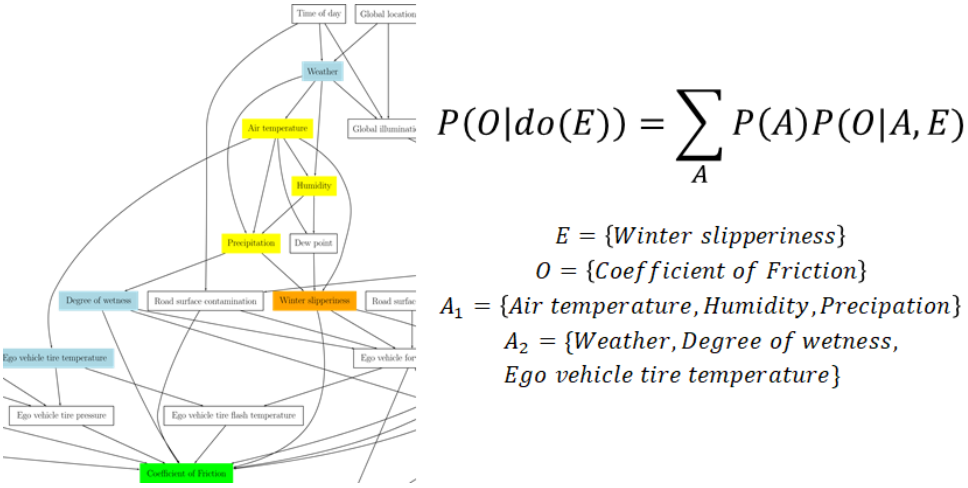


Abbildung 114: Darstellung verschiedener minimaler Mengen von Knoten (links), die die Berechnung eines kausalen Effektes über die “Backdoor adjustment” Formel (rechts) ermöglichen. An dieser Stelle wird der Effekt der Winterglätte auf den Reibwert betrachtet. (© DLR e.V.)

Im Zuge der Evaluation der Modellqualität der mit Daten angereicherten Kausalgraphen wurden Indikatorfunktionen definiert, die als notwendige Bedingung für die Korrektheit der modellierten Graphstruktur betrachtet werden können. Diese können wiederum im zuvor beschriebenen iterativen Prozess der Modellentwicklung zur Falsifizierung einzelner Modellabschnitte genutzt werden und helfen dabei bei der Annäherung von Expertenwissen und Beobachtungsdaten im Modell.

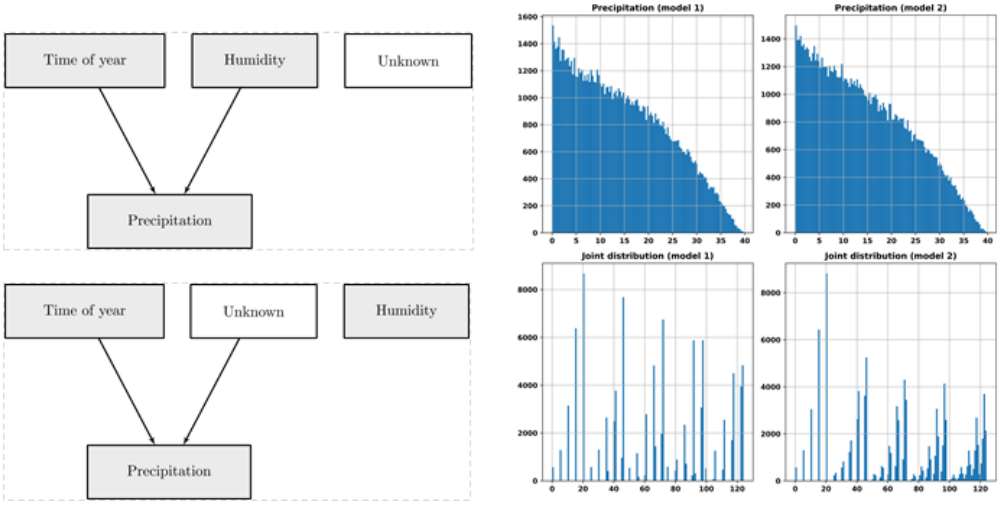


Abbildung 115: Vergleich angenommener Ursache-Wirkung Beziehungen. Trotz gleicher Wahrscheinlichkeitsverteilung der Wirkung enthüllt die Betrachtung der Gesamtverteilung einen Unterschied, der durch Kausalitäten strukturiert sichtbar gemacht werden kann. (© DLR e.V.)

3.1.1.6.2.2 Der Informations-Zweig

Die Hauptaufgabe des Informations-Zweigs ist die Abspeicherung und Bereitstellung von Informationen, welche wir in Wissen und Daten differenzieren. Die anderen Zweige der Kritikalitätsanalyse greifen dauerhaft auf Daten und Wissen zu, beispeilsweise um die Relevanz von Kritikalitätsphänomenen zu schätzen. Weiterhin wird gewonnenes Wissen (bspw. initiale Wirkzusammenhänge hinter Kritikalitätsphänomenen anhand von Experteninterviews) in der Wissensbasis gespeichert. Auch Daten (wie abstrakte Szenarien) können dort abgelegt werden.

Als zentrales Werkzeug für die Wissensbasis werden Ontologien genutzt. Sie können Wissen über kategorischen Konzepten (d.h. Fakten) darstellen und diese mit Daten (d.h. konkreten Instanzen über den Fakten) verknüpfen. Ontologien können sowohl auf informeller Ebene als auch stark formalisiert genutzt werden. Ein Beispiel für Ersteres ist das sogenannte 6-Ebenen-Modell, welches erstmals in PEGASUS entwickelt wurde und im Rahmen von VVMethoden für den urbanen Raum angepasst wurde [46]. Basierend darauf konnte in VVMethoden mit der Automotive Urban Traffic Ontology (A.U.T.O.) eine Formalisierung des 6-Ebenen-Modells erreicht werden [67]. Über automatisiertes Schlussfolgern anhand der gegebenen Fakten kann neues Wissen aus Daten generiert werden und so den Informations-Zweig anreichern. Ein Beispielausschnitt aus A.U.T.O. ist in Abbildung 116 gegeben.

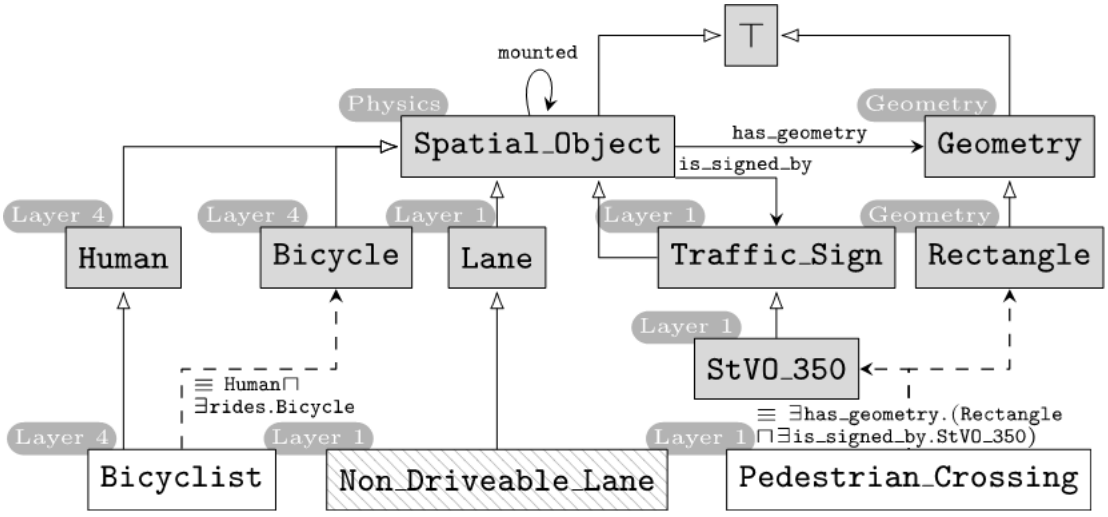


Abbildung 116: Beispielausschnitt aus A.U.T.O. zu Fußgängerüberwegen und Radfahrenden (© DLR e.V.)

Letztendlich ermöglichen Ontologien somit das Abstrahieren der realen Welt und dienen in der Kritikalitätsanalyse als zentrales Element, um über Artefakte der realen Welt zu argumentieren – bspw. können Kritikalitätsphänomene [67] sowie Wirkzusammenhänge [65] ontologiebasiert definiert werden.

Neues Wissen im Informations-Zweig kann hauptsächlich über zwei Wege gewonnen werden: Einerseits über Datenanalysen (bspw. mit Kritikalitätsmetriken [65]) und andererseits über deduktives Folgern aus bereits vorhandenem Wissen. Somit wachsen die in der Kritikalitätsanalyse gewonnen Informationen im Laufe der Methode an.

3.1.1.6.2.3 Der Szenarien-Zweig

Der Szenarien-Zweig bettet die Artefakte der Kritikalitätsanalyse, insbesondere die CP und deren CR, in einen szenarienbasierten Entwicklungsprozess ein. Dort wird die Frage beantwortet

> Wie werden Szenarien in der Kritikalitätsanalyse verwendet?

In der relevanten Literatur werden üblicherweise vier Abstraktionslevel der Szenarienbeschreibung unterschieden: funktional > abstrakt > logisch > konkret (siehe Abbildung 117).

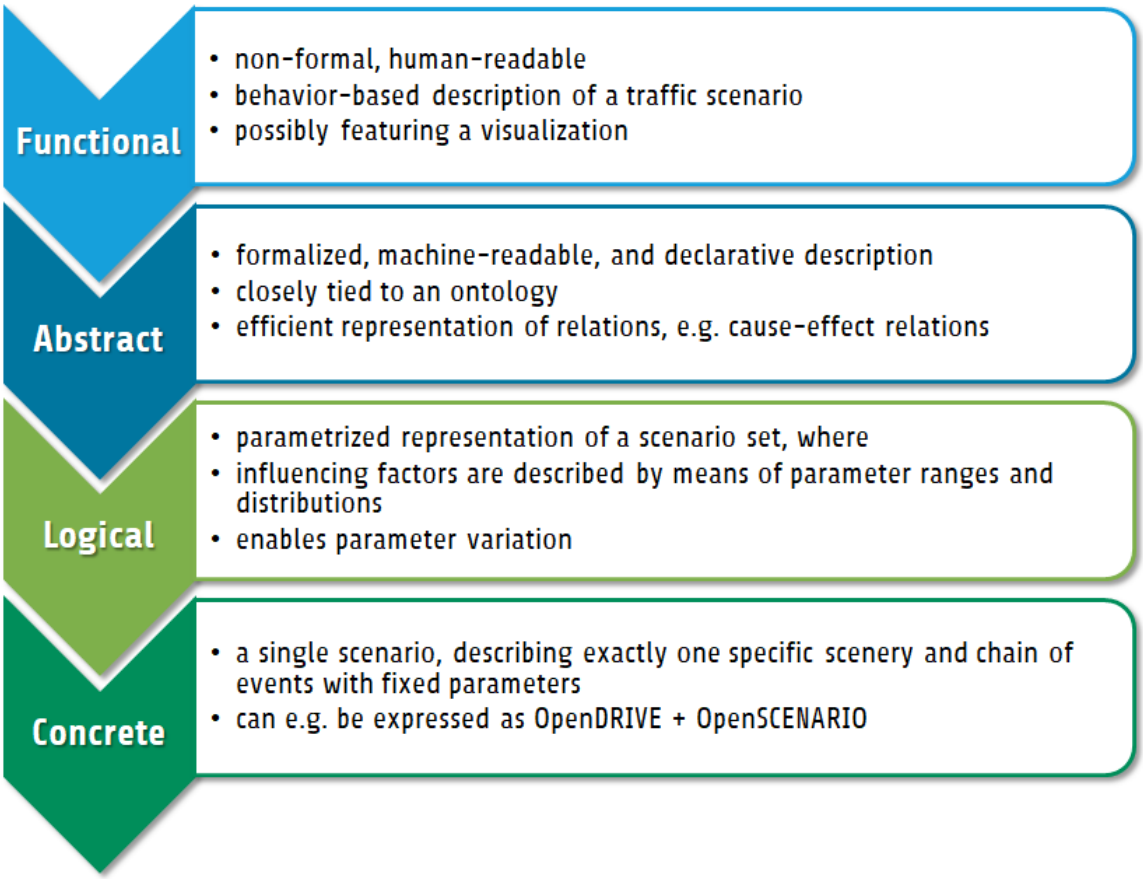


Abbildung 117: Abstraktionsstufen der Szenarienbeschreibung (© Neurohr et al. [57])

Die Kritikalitätsanalyse benutzt hierbei abstrakte Szenarien um die CP und deren CR in den Kontext des szenarienbasierten Ansatzes einzubetten [57] [69]. Diese abstrakten Szenarien können dann bei Bedarf weiter konkretisiert werden, bspw. zu logischen oder konkreten Szenarien, und an anderer Stelle gewinnbringend eingesetzt werden, z.B. bei der Gefährdungsanalyse oder zur Verifikation der AF. Abbildung 118Abb. 14 zeigt ein abstraktes Kreuzungsszenario mit komplizierter Vorfahrtsregelung und kreuzendem Fußgänger.

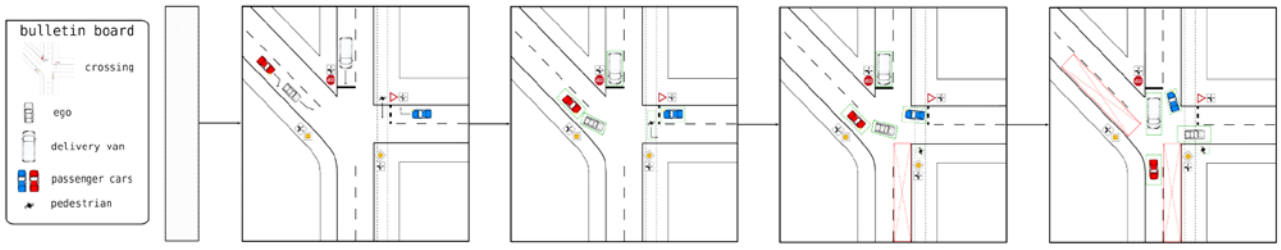


Abbildung 118: Ein abstraktes Kreuzungs-Szenario, vgl. [70], spezifiziert als Traffic Sequence Chart [69].

Sobald Echtweltdaten oder synthetische Daten integriert werden, werden auch logische und konkrete Szenarien in der Kritikalitätsanalyse eingesetzt. Insbesondere zur Quantifizierung von Kritikalität werden Kritikalitätsmetriken auf konkreten Szenarien evaluiert [65].

3.1.1.6.2.4 Beiträge zur Gesamtmethode

Die Beiträge einer Kritikaltitätsanalyse für den weiteren Entwicklungsprozess sowie zur Sicherheitsargumentation sind zahlreich. Für Details verweisen wir auf [64] Abschnitt 6.

Eine Auswahl der Beiträge zum Entwicklungsprozess der AF:

- Die CP und CR welche während der Kritikalitätsanalyse identifiziert und formalisiert sowie modelliert und validiert wurden, dienen als wertvolle Informationsquelle in einer anschließenden Hazard Analysis and Risk Assessment (HARA).
- Darüber hinaus können CR die Basis für Anforderungen an das AF-Verhalten bilden
- Abstrakte Szenarien welche CP und deren CR enthalten können zur Validierung der AF auf Verhaltenslevel genutzt werden.

Auch zur Sicherheitsargumentation tragen die Artefakte der Kritikalitätsanalyse bei, zum Beispiel:

- Die CP und deren CR tragen zur Identifikation und Evaluierung von „Triggering Conditions“ im Sinne der ISO 21448 bei [48]
- Kritikalitätsmetriken ermöglichen die Quantifizierung von Evidenzen in der Sicherheitsargumentation
- Falls die Kritikalitätsanalyse bis zur angestrebten Saturierung der Artefakte (insbesondere der CP und CR) durchgeführt wurden, so dass dies als starkes Argument zur Erfüllung der „Safety of the intended Functionality“ (SOTIF) aufgeführt werden

Zusammenfassend arbeiten die Resultate einer für die beabsichtigte OD durchgeführten Kritikalitätsanalyse dem Entwicklungsprozess von einer Klasse von AF sowie der zur Freigabe benötigten Sicherheitsargumentation zu.

3.1.1.7 Fähigkeitenanalyse und Verhaltensspezifikation

3.1.1.7.1 Motivation und Überblick

Eine der wesentlichen Herausforderungen bei der Absicherung automatisierter Fahrsysteme stellt die systematische Beschreibung und Analyse des Verkehrskontextes dar. In den vorherigen Kapiteln wurden Ansätze aus VVMethoden dargestellt, die sich zunächst mit der strukturierten Beschreibung der relevanten Elemente in diesem Verkehrskontext befassen. In diesem Abschnitt werden Beiträge aus VVMethoden zusammengefasst, welche die Frage “Welches Verhalten soll ein automatisiertes Fahrsystem in seiner Umgebung aufweisen?” konkretisieren. Darüber hinaus werden Ansätze zur Beantwortung dieser Fragestellung gezeigt.

Die explizite Betrachtung des aufzuweisenden Verhaltens (im Folgenden „Sollverhalten“) und die Formulierung entsprechender Verhaltensanforderungen ist notwendig, da ein Nachweis hinreichender Sicherheit über die Abwesenheit unzumutbarer Risiken erfolgt. Risiko wird in der Sicherheitstechnik definiert als Kombination der Schwere und Auftretenswahrscheinlichkeit eines Schadens. Im Bezug auf das Verhalten eines automatisierten Fahrsystems kann ein Schaden nur auf der Gesamtsystemebene entstehen. Infolgedessen werden Fahrmanöver und ihre potentiellen Auswirkungen beschrieben sowie kausale Zusammenhänge zum entsprechenden (szenarienabhängigen) Kontext beschrieben. Neben der Betrachtung von Risiken, welche sich auf

potentielle physische Verletzungen beschränken, ist der explizite Nachweis zu führen, warum ein automatisiertes Fahrsystem sich konform zu den geltenden Verkehrsregeln verhalten wird. Daher werden in diesem Abschnitt auch Ansätze aus VVMethoden gezeigt, welche den Bezug des spezifizierten Sollverhaltens zu den zugrundeliegenden Verkehrsregeln explizit beschreibbar machen.

In Bezug auf beide Ziele - Sicherheit und Konformität - leistet die explizite Spezifikation von Sollverhalten einen Beitrag gegenüber der rein technischen Betrachtung von Systemfunktionen, da die in der ISO 21448 beschriebenen Spezifikationsinsuffizienzen so systematischer analysiert werden können. Eine Spezifikationsinsuffizienz ist nach ISO 21448 eine “Spezifikation - möglicherweise unvollständig - die zu gefährlichem Verhalten […] beiträgt, wenn sie durch einen auslösenden Umstand aktiviert wird” (übersetzt von Salem, 2024). Da die Spezifikation von Systemfunktionen vorrangig dem Ziel folgt, dass das automatisierte Fahrsystem auf Gesamtsystemebene ein Verhalten aufweist, ist auch das Sollverhalten für eine systematische Identifikation möglicher Insuffizienzen explizit zu spezifizieren. Bei der Entwicklung und Absicherung automatisierter Fahrsysteme ist vor dem Hintergrund der o.g. Ziele der Nachweis zu führen, warum ein Fahrsystem sich sicher und konform in einem definierten Verkehrskontext verhält. Die im folgenden vorgestellten Ansätze unterstützen die Analyse von Spezifikationsinsuffizienzen durch eine explizite Beschreibung von Sollverhalten.

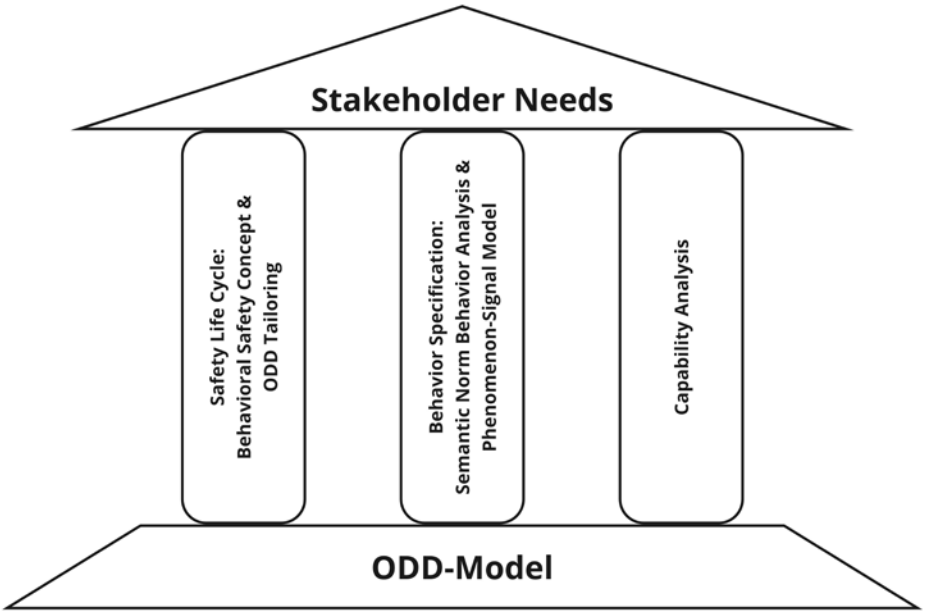


Abbildung 119: Überblick der Themen des Kapitels “Fähigkeiten-Analyse und Verhaltensspezifikation”

Abbildung 119 fasst die in diesem Abschnitt diskutierten Inhalte zusammen. Die Basis dieses Abschnitts bildet eine systematische Beschreibung relevanter Kontextelemente und ihrer Zusammenhänge (ODD-Model), welche in den vorherigen Kapiteln eingeführt wurde. Darauf aufbauend wird in Kapitel 3.1.1.7.2 die Semantische Normverhaltensanalyse eingeführt. Die Methode zielt grundsätzlich auf die explizite Einbeziehung von Stakeholder Needs (Erwartungen beteiligter Interessengruppen) in das spezifizierte Sollverhalten. Die Anwendung der Methode beschränkt sich zunächst auf die explizite (beispielhafte) Einbeziehung von Verkehrsregeln. Kapitel 3.1.1.7.3 geht eingehend auf die formale Modellierung von Sollverhalten mithilfe des Phänomen-Signal-Modells ein. Mit einem Fokus auf das Ziel Sicherheit wird in Kapitel 3.1.1.7.4 ein

Beitrag zur Erstellung von Verhaltenssicherheitskonzepten vorgestellt, welcher die Anwendung des Risk Management Core auf die Verhaltensspezifikation darlegt. Abschließend wird in Kapitel 3.1.1.7.5 auf den Einsatz des Konzeptes der Systemfähigkeiten im Kontext des automatisierten Fahrens eingegangen.

3.1.1.7.2 Semantische Normverhaltensanalyse

Die Beiträge der Semantischen Normverhaltensanalyse sind bereits in einer wissenschaftlichen Veröffentlichung [71] formuliert. Der folgende Textbaustein ist dieser Veröffentlichung entnommen.

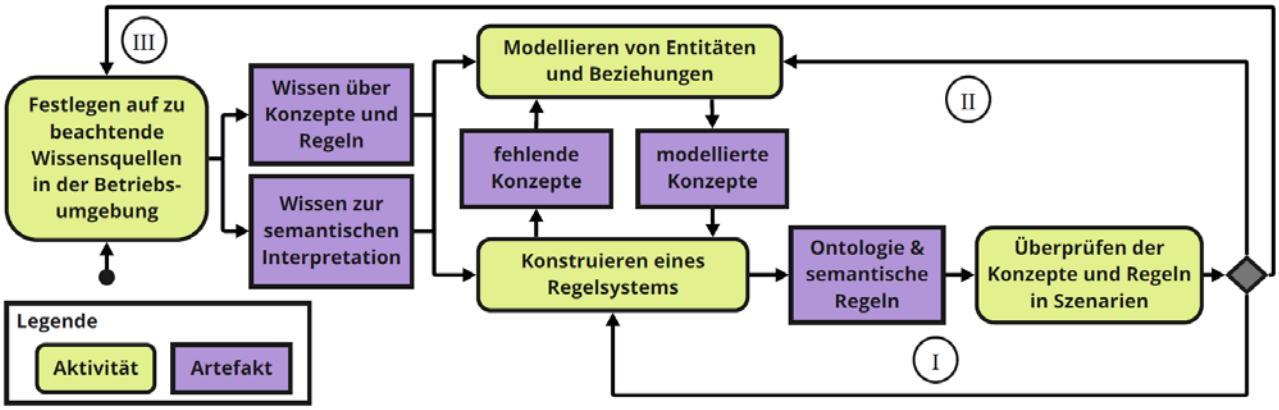


Abbildung 120: Darstellung des Vorgehens bei der semantischen Normverhaltensanalyse . Iterationen I, II und III werden durchlaufen, wenn die Überprüfung des inferierten Sollverhaltens Fehler im Regelsystem, Fehler bei den modellierten Konzepten oder Fehler bei der Auswahl der Wissensquellen feststellt. Fehlerhaftes Verhalten bedeutet: nonkonformes oder unsicheres Verhalten.

Abbildung 120 stellt das Vorgehen der semantischen Normverhaltensanalyse dar. Im ersten Schritt werden die genutzten Wissensquellen für die Analyse des Normverhaltens gewählt (z.B. die StVO). Diese Wissensquellen können Informationen zu Konzepten und Regeln sowie Methoden zum Umgang mit den gewählten Wissensquellen beinhalten. Wissensquellen sind im Kontext der Betriebsumgebung auszuwählen und zu analysieren. Die Betriebsumgebung wird hier als Summe von Bedingungen verstanden, unter denen ein automatisiertes Fahrzeug erwartbar und zulässig betrieben wird. Zur Modellierung des Norm- und Sollverhaltens müssen zunächst die Elemente, die für die formale Beschreibung der Verhaltensregeln notwendig sind, aus den Wissensquellen herausgearbeitet werden. Während in den meist natürlich-sprachlich dokumentierten Quellen auch implizites Wissen enthalten ist, kann mit Hilfe expliziter Konzepte erklärbar und rückverfolgbar geschlussfolgert werden. Zum Beispiel verwendet die StVO Konzepte wie *Fahrstreifen*. Dabei ist ein Fahrstreifen immer Bestandteil einer *Fahrbahn*. Das Wissen darüber, dass das Befahren eines Fahrstreifens einer Fahrbahn immer auch das Befahren der Fahrbahn bedingt, erscheint zunächst trivial, kann aber bei der formalen Beschreibung eine wesentliche Schlussfolgerung sein.

Wissen über Konzepte und Regeln stammt häufig aus Wissensquellen, die Expertenwissen zur semantischen Interpretation voraussetzen. Daher sind zusätzlich Wissenquellen notwendig, die Methoden zum Umgang mit Domänenwissen beschreiben. Diese Methoden werden genutzt, um die Wissensquellen systematisch auf enthaltenes Wissen zu untersuchen und die Konzepte und Regeln zu formalisieren. Methodisches sowie domänenbezogenenes Expertenwissen und damit verbundene semantische Interpretationen sind oft notwendig, weil Entitäten, Relationen und Regeln nicht immer explizit dokumentiert sind. Ohne Interpretation impliziter zu expliziten Konzepten wäre eine formale Repräsentation semantischer Beziehungen nicht möglich. Das auf

dem VVMethoden-Abschlussevent gewählte Beispiel erfordert etwa die Repräsentation des Konzepts von „erkennbar querenden zu Fuß Gehenden“. Die StVO als Wissensquelle gibt keinen unmittelbaren Aufschluss darüber, welche Bedingungen an dieses Konzept geknüpft sind. Domänen-Expert*innen könnten hier zum Beispiel Gerichtsurteile heranziehen, um eine Interpretation zu stützen. Eine Anbindung der Wissensmodellierung an existierendes Domänenwissen durch die flexible Wahl der Wissensquellen sowie der Methoden zur semantischen Interpretation ist ein zentrales Ziel der semantischen Normverhaltensanalyse. Der Ansatz stellt so die Anforderung an Domänen-Expert*innen, die Wissensquellen bezüglich enthaltener Konzepte und Regeln zu trennen. Die formale Strukturierung von Konzepten und Regeln ermöglicht eine formale Überprüfbarkeit der modellierten Verhaltensregeln hinsichtlich ihrer Konsistenz. Zur formalen Repräsentation des natürlich-sprachlichen Wissens werden in der semantischen Normverhaltensanalyse Ontologien verwendet. Um diese Ontologien zur Verhaltensspezifikation nutzen zu können, werden Entitäten, deren Beziehungen sowie Inferenzregeln aus den zugrundeliegenden Wissensquellen modelliert. Die Konzeptualisierung von Entitäten und Beziehungen (Schritt 2) sowie die Konstruktion von Regeln (Schritt 3) bilden einen iterativen Prozess, da Konzepte in teilweise implizit repräsentiertem Wissen erst bei der Regelkonstruktion identifiziert werden können

Verifiziert wird der erzeugte Regelkatalog in einem letzten Analyseschritt, in dem die Regeln auf alle betrachteten Szenarien angewendet werden. Dieser Schritt kann zum Beispiel mithilfe eines Phänomen-Signal-Modells [72] [73] durchgeführt werden. Mit der semantischen Normverhaltensanalyse wird zunächst nur eine systematische Ableitung von Verhaltensregeln für Szenen [28] eines funktionalen Szenarios [74] [75] beabsichtigt. Das Sollverhalten setzt sich auf der Beschreibungsebene eines funktionalen Szenarios aus den angewendeten Verhaltensregeln zusammen. Aus der Verifikation ergeben sich im Rahmen der semantischen Normverhaltensanalyse (Abbildung 120) drei unterschiedliche Arten möglicher Fehlerfälle, die durch drei entsprechende Iterationsschleifen adressiert werden. Fehlerfälle bezeichnen eine Abweichung des aus dem spezifizierten Regelkatalog resultierenden Verhaltens von dem durch die Analyse der Wissensquellen vorgegebenen Verhalten und damit nonkonformes oder unsicheres Verhalten. Die erste Iteration (I) wird durch einen Fehlerfall aufgrund unzureichend definierter Regeln bedingt. Unzureichend bedeutet hier widersprüchlich oder nicht ausreichend detailliert. Ziel dieser Schleife ist die Erzeugung eines konsistenten Regelkatalogs. Der Eintritt in die zweite Iterationsschleife (II) wird durch fehlende Konzepte ausgelöst. Diese Schleife ist nötig, da selbst in einem konsistenten Regelkatalog festgestellt werden kann, dass die Konzeptualisierung für ein Szenario nicht hinreichend vollständig ist. Das Ziel der Schleife ist die Korrektheit des Regelkatalogs in Bezug auf die untersuchten Szenarien. In der dritten Schleife (III) kann eine in Bezug auf die Szenarien und Wissensquellen hinreichend vollständige Ontologie der Konzepte und ein widerspruchsfreier Regelkatalog vorliegen. Falls dennoch in Frage steht, ob das geschlussfolgerte, regelkonforme Verhalten dem tatsächlich gewünschten Sollverhalten entspricht, können die Wissensbasis geprüft und neue Quellen hinzugezogen werden. Da Szenarien für die Ableitung von Verhaltensnormen genutzt werden, ist die Repräsentativität des Szenarienkatalogs maßgeblich verantwortlich für die Validität des formalisierten Sollverhaltens innerhalb einer Betriebsumgebung. Die Überprüfung der Übertragbarkeit formalisierter Konzepte und Regeln von den analysierten Szenarien auf den offenen Kontext ist nicht Bestandteil des vorgeschlagenen Ansatzes. Grenzen des Ansatzes können daher in Hinblick auf die Repräsentativität des genutzten Szenarienkatalogs und die Validität der verwendeten Wissensquellen identifiziert werden. In Bezug auf die verwendeten Wissensquellen bezieht sich die Validität auf die Akzeptanz der Auswahl aus der Sicht relevanter Stakeholder in der Betriebsumgebung.

3.1.1.7.3 Phänomen-Signal-Modell

Die Beiträge des Phänomen-Signal-Modells sind bereits in einer (deutschen und englischen) Veröffentlichung [72] [73] formuliert. Folgende Textbausteine sind (größtenteils) aus der deutschen Veröffentlichung übernommen.

Mit dem Phänomen-Signal-Modell (PSM) werden die Entscheidungsmöglichkeiten eines automatisierten Fahrsystems abhängig von situationsbedingt empfangenen Signalen über den umgebenden Verkehrsraum und das Verhalten anderer Verkehrsteilnehmer dargestellt. Von den jeweiligen regelbasierten Entscheidungsmöglichkeiten abhängige Veränderungen der Verkehrssituation werden daraus gefolgert.

Zudem werden die dem Fahrzeug vorliegenden Informationen und daraus abgeleiteten Entscheidungsmöglichkeiten überprüft und der Graph für diese weiterentwickelt. Der Weg dahin führt über Formalisierung von externem Verhalten, Wissen und Signalen. Das Konzept eröffnet Möglichkeiten zur Darstellung und Auswertung des Verhaltens des Fahrzeugs und daraus resultierender Szenarienverläufe. Dies soll für die Implementierung des gewünschten Fahrzeugverhaltens, sowie dessen Absicherung und Verifikation genutzt werden. So wurde in VVMethoden an einer computergestützten Generierung und Auswertung der PSM-Graphen gearbeitet. Dies ist für eine praxisgerechte Anwendung des Konzepts notwendig, um die in der Realität gegebene große Zahl von Verlaufs- und Variationsmöglichkeiten des Szenarios bewältigen zu können.

Ein Phänomen-Signal-Modell stellt damit formale Werkzeuge bereit, Sollverhalten explizit zu modellieren. Da die Ausführungen zum erarbeiteten Formalismus nicht zielführend im Rahmen dieses Abschlussberichtes sind, wird in Abbildung 121 illustrativ ein PSM-Graph dargestellt.

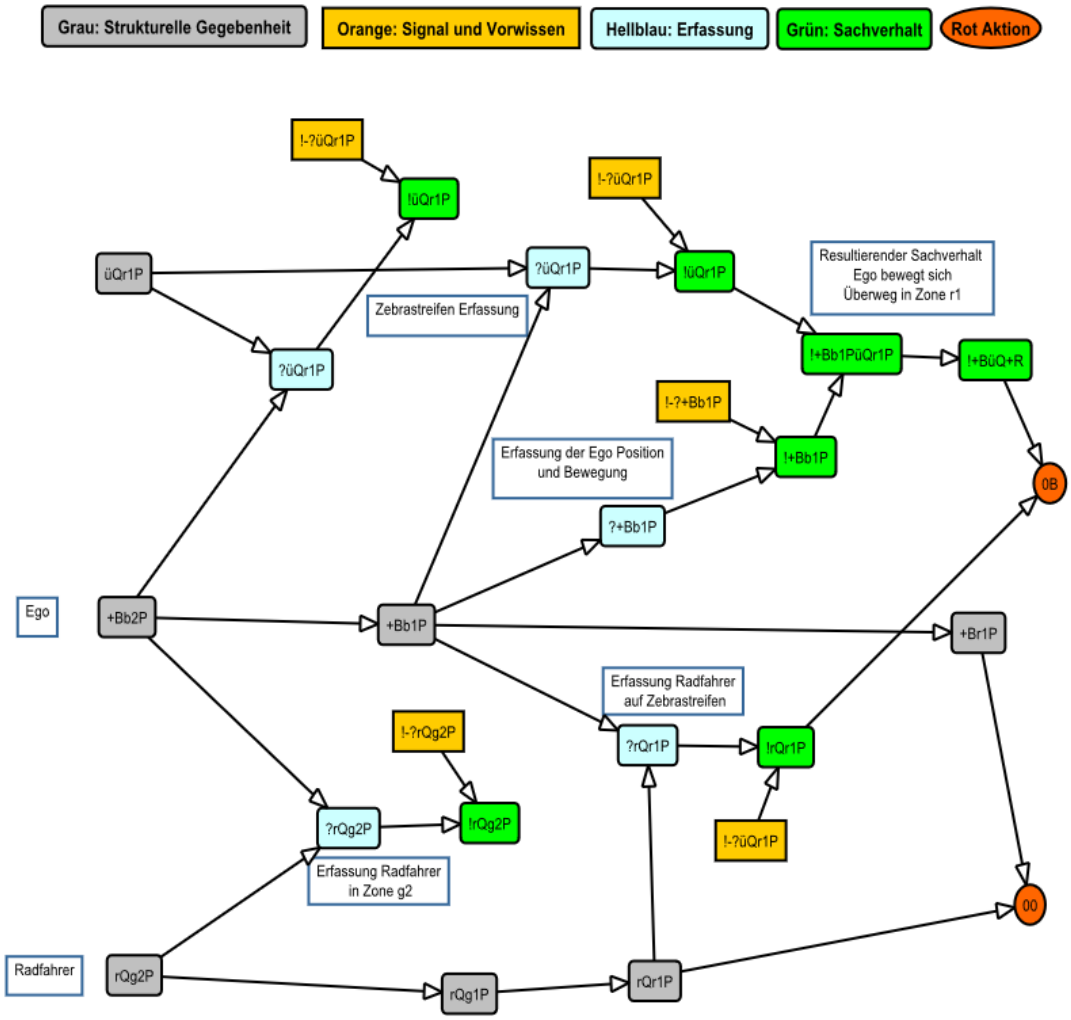


Abbildung 121: Beispielhafter PSM-Graph für ein Szenario an einer T-Kreuzung mit einem Radfahrer am Fußgängerüberweg

3.1.1.7.4 Verhaltenssicherheitskonzept

In Kapitel 3.1.1.2.5 wurde ein grundlegendes Vorgehen für die systematische Analyse, Bewertung und Behandlung von Risiken automatisierter Fahrsysteme - der Risk Management Core - eingeführt. Wir verwenden den Risk Management Core, um zu zeigen, wie das grundlegende Vorgehen auf das Risikomanagement im Zusammenhang mit der Spezifikation des Verhaltens automatisierter Fahrsysteme angewendet werden kann. Die ISO 21448 verlangt eine Argumentation für die Abwesenheit unangemessener Risiken aufgrund funktionaler Unzulänglichkeiten. Funktionale Unzulänglichkeiten werden entweder als Leistungs- oder Spezifikationsunzulänglichkeiten definiert. Während die ISO 21448 allgemeine Richtlinien zur Identifizierung solcher Unzulänglichkeiten beschreibt, stellt sie keinen Hinweis auf eine Methode bereit, welche potentielle Unzulänglichkeiten der Verhaltensspezifikation adressiert. In diesem Abschnitt stellen wir eine risikobasierte Verfeinerung der Verhaltensspezifikation vor, die zu einem Verhaltenssicherheitskonzept führt. Dieses Verfahren wurde detailliert in einer wissenschaftlichen Veröffentlichung beschrieben [76].

Abbildung 122 zeigt ein Vorgehen zur Anwendung des Risk Management Core zur risikobasierten Verfeinerung der Verhaltensspezifikation.

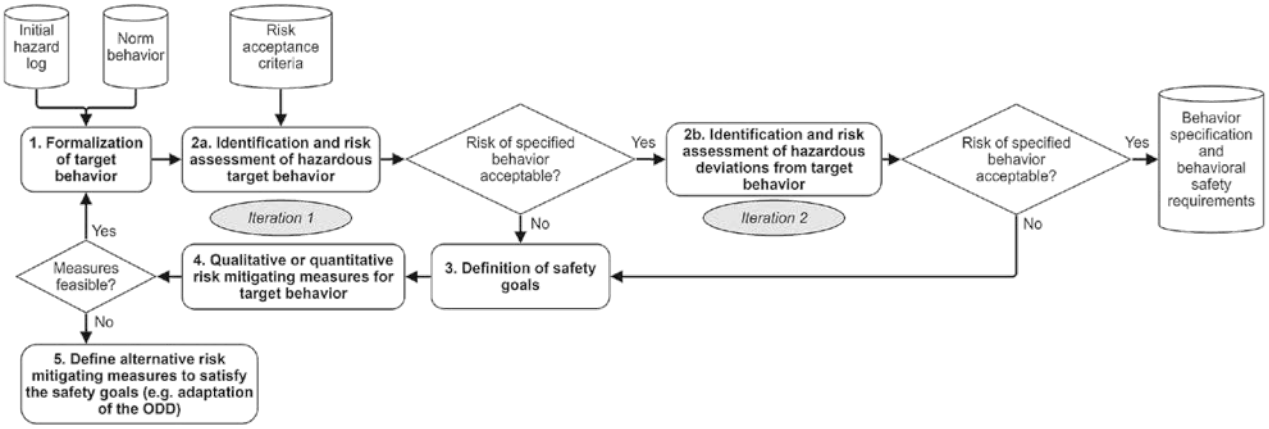


Abbildung 122: Methode zur risikobasierten Verfeinerung der Verhaltensspezifikation auf Basis des Risk Management Cores

Zur Umsetzung von Schritt 1 wurde ein möglicher Ansatz in VVMethoden entwickelt, der es erlaubt Design-Annahmen und Entscheidungen in einer Verhaltensspezifikation explizit zu beschreiben. Das ”Phänomen-Signal-Modell” (PSM) ist ein Werkzeug zur formalen Beschreibung von Sachverhalten und Regeln, die das Sollverhalten eines automatisierten Fahrsystems im Straßenverkehr beschreiben. Zusätzlich wurde die "Semantische Normverhaltensanalyse" als ein Ansatz zur Ableitung solcher Sachverhalte und Regeln auf Basis von Stakeholder Needs entwickelt. Die Kombination von Sachverhalten und Regeln in einer Graphen-Darstellung ergibt eine (semi-)formale Spezifikation des Sollverhaltens. Neben der Berücksichtigung von Stakeholder Needs wird bereits vorhandenes Wissen bzgl. bekannter Gefährdungen in der Methode berücksichtigt (Initial Hazard Log). Diese bekannten Gefährdungen werden durch folgende Schritte zur Gefährdungsidentifikation angereichert. Der erste Schritt der Formalisierung des Sollverhaltens unterstützt eine risikobasierte Verfeinerung der Verhaltensspezifikation insofern, dass er eine explizite Repräsentation von gefährlichem Verhalten (d.h. Verhalten, das zu gefährlichen Ereignissen führt) ermöglicht. Darüber hinaus können so auslösende Umstände (triggering conditions) und funktionale Unzulänglichkeiten identifiziert und beschrieben werden. Diese Unzulänglichkeiten müssen explizit mit Maßnahmen zur Risikominderung (qualitativ und quantitativ) adressiert werden, wenn sie zu unzumutbaren Risiken führen. Die formale Darstellung von Sollverhalten, die das Phänomen-Signal-Modell (PSM) bietet, erfüllt diese Anforderungen, da die Darstellung auf Sachverhalten und Regeln beruht, welche einen kausalen Zusammenhang zwischen der Betriebsumgebung und einem spezifizierten Manöver beschreiben. Zusätzliche Sachverhalte und Regeln lassen sich darüber hinaus systematisch aus erforderlichen Risikominderungsmaßnahmen ableiten.

Schritt 2a (Abbildung 122) befasst sich mit der Identifikation von gefährlichem Sollverhalten. Wenn wir das Sollverhalten als eine Menge T und gefährliches Verhalten eine Menge H beschreiben, dann zielt dieser Schritt darauf ab, das verhaltensbezogene Risiko $r_{beh,t}$ zu identifizieren und zu analysieren, das sich aus T∩H ergibt. Das verhaltensbezogene Risiko ist dann zu berechnen entsprechend einer Funktion f mit $r_{beh,t} = f(T \cap H)$. Das Ergebnis wird im Rahmen eines Vergleichs des (geschätzten) tatsächlichen Risikos mit dem akzeptablen Risiko r_{rac} bewertet. Es ist zu beachten, dass eine solche skalare Bewertung dazu dient einen Vergleich zu veranschaulichen, während tatsächliche und akzeptierte Risiken potenziell eine höhere Dimensionalität aufweisen. Ist $r_{beh,t} > r_{rac}$ ist eine Risikominderung erforderlich.

Sicherheitsziele werden definiert (vgl. Abbildung 122, Schritt 3), um den Risikominderungsbedarf qualitativ und quantitativ zu erfassen. Die Gütekriterien zur Erbringung der Risikominderung sind sowohl für die nominale Risikominderung als auch für die Sicherheitsintegrität zu spezifizieren. Für diesen Schritt ist nicht unbedingt eine Definition neuer Sicherheitsziele erforderlich. Falls bereits umfangreiches Wissen über Sicherheitsziele vorhanden ist, kann die Methode zu Verfeinerung bestehender Sicherheitsziele verwendet werden.

Sicherheitsziele werden durch die Spezifikation von Sicherheitsmaßnahmen erreicht (vgl. Abbildung 122, Schritt 4). Zur Definition von Sicherheitsmaßnahmen auf der Ebene der Verhaltensspezifikation führen wir das Konzept der verhaltensbezogenen Sicherheitsanforderungen (Verhaltenssicherheitsanforderungen) ein. Verhaltenssicherheits-anforderungen sind eine Spezialisierung der funktionalen Sicherheitsanforderungen, die das Verhalten eines „System of Systems“ in einem szenariospezifischen Kontext spezifizieren. Im Gegensatz dazu beziehen sich die traditionellen funktionalen Sicherheitsanforderungen (insbesondere im Kontext der ISO 26262) auf ein „System of Interest“ in seiner gesamten Betriebsumgebung. Mit Hilfe des Konzepts der Systemfähigkeiten stellen wir einen Zusammenhang zwischen Verhaltenssicherheitsanforderungen und Architekturelementen her. Die Verwendung von Systemfähigkeiten als Architekturbeschreibungselemente, die für ein bestimmtes Sollverhalten erforderlich sind, wurde in der wissenschaftlichen Literatur bereits untersucht [77] [78] [79] [80]. Hierbei wurden Anforderungen im Kontext der funktionalen Sicherheit spezifiziert und Fähigkeiten zugeordnet. Wir hingegen fokussieren uns auf den Aspekt der Verhaltenssicherheit (SOTIF) und nutzen Fähigkeiten daher als Mittel, um Verhaltenssicherheitsanforderungen zu abstrahieren.

Im Rahmen der funktionalen Sicherheit (nach ISO 26262) ist ein Argument vorzulegen, warum kein unangemessenes Risiko von Gefährdungen durch fehlerhaftes Verhalten von elektrischen und/oder elektronischer (E/E) Systeme ausgeht. Für SOTIF gilt jedoch die Abwesenheit eines unangemessenen Risikos aufgrund von Gefährdungen, die sich aus funktionalen Unzulänglichkeiten der vorgesehenen Funktionalität oder deren Implementierung resultieren. Da eine Spezifikation eines sicheren Sollverhaltens im Kontext der funktionalen Sicherheit angenommen wird, müssen SOTIF-bezogene Aktivitäten (unter anderem) zu einer Spezifikation des sicheren Sollverhaltens führen. Verhaltenssicherheitsanforderungen könnten somit die „Vehicle-Level SOTIF Strategy“ (VLSS) unterstützen, die ausschließlich Anforderungen für die beabsichtigte Funktionalität auf Fahrzeugebene enthält. Insbesondere die explizite Spezifikation von Risikominderung und Sicherheitsintegrität ist für die Sicherheitsargumentation in diesem Kontext wesentlich. Darüber hinaus könnte eine systematische Beschreibung des Sollverhaltens Aktivitäten im Lebenszyklus der funktionalen Sicherheit wie zum Beispiel eine systematische Gefährdungsidentifikation [81] [82] und eine anschließende Spezifikation von Sicherheitszielen [80] unterstützen.

Der Umfang unserer Beispielanwendung des Risk Management Core bezieht sich nur auf die Verhaltensspezifikation. Daraus folgt, dass (z. B. wirtschaftlich oder technologisch) nicht durchführbare Maßnahmen zur Risikominderung als Maßnahmen in der ersten Iteration definiert werden können. Wenn dies der Fall ist, können alternative Maßnahmen zur Anpassung des Sollverhaltens festgelegt werden (vgl. Abbildung 122 Schritt 5). Solche Maßnahmen könnten zum Beispiel Modifikationen der Operational Design Domain umfassen.

Schließlich wird Iteration 1 (vgl. Abbildung 122) durch die Integration der spezifizierten Risikominderungsmaßnahmen in die Verhaltensspezifikation abgeschlossen. Iteration 1 befasst sich also mit der Minderung von $r_{beh,t} = f(T \cap H)$ auf einen akzeptablen Wert.

Unter der Annahme, dass es einen Punkt gibt, an dem das Restrisiko, das sich aus dem Sollverhalten des automatisierten Fahrsystems ergibt, einen akzeptablen Wert erreicht, beginnt Iteration 2. Die ISO 21448 definiert, dass auslösende Umstände, die zu Abweichungen vom Sollverhalten führen können (vgl. Abbildung 122, Schritt 2b) zu analysieren sind. Wenn die Abweichungen als gefährlich eingestuft werden, muss das aus einem solchen Verhalten resultierende Risiko $r_{beh,d} = f(H \setminus T)$ quantifiziert werden. Um Iteration 2 erfolgreich zu beenden, muss das aus dem Sollverhalten resultierende Risiko unter dem akzeptablen Risikoniveau liegen ($r_{beh,t} + r_{beh,d} < r_{rac}$). Wenn die Risikobewertung zeigt, dass mindestens ein Risikoakzeptanzkriterium verletzt wird, ist eine weitere Risikominderung erforderlich. Risiken, die aus spezifizierten Sicherheitsmaßnahmen ergeben (vgl. [83]) entstehen, werden zwangsläufig durch einen erneuten Einstieg in Iteration 1 analysiert. Wenn alle Risikoakzeptanzkriterien durch die Verhaltensspezifikation erfüllt sind - einschließlich Risikominderung und Sicherheitsintegrität - kann ein Verhaltenssicherheitskonzept erstellt werden, welches die identifizierten Gefährdungen und spezifizierte Maßnahmen im Rahmen des Sollverhaltens beschreibt.

3.1.1.7.5 Identifikation und Konsolidierung von Systemfähigkeiten

Eine spezifische Herausforderung im Kontext automatisierter Fahrzeugsysteme ist die Spezifikation und der Nachweis des sicheren Verhaltens der Systeme in ihrer Betriebsumgebung. In VVMethoden wurde ein szenarienbasierter Entwicklungs- und Absicherungsansatz als Mittel zur Komplexitätsbeherrschung verfolgt. Derartige Ansätze zielen darauf ab, das Sollverhalten des zu entwickelnden automatisierten Fahrzeugs zunächst im Rahmen des Entwurfs und der Entwicklung in ausgewählten Szenarien zu beschreiben (vgl. z.B. [84] [85] [86]). Das definierte Sollverhalten dient der Formulierung von Anforderungen, die dann im Rahmen der Verifikation und Validierung überprüft werden, um zunächst nachzuweisen, dass von der Spezifikation des Systems kein unangemessenes Risiko ausgeht.

Für die Ableitung eindeutig nachverfolgbarer Verifikations- und Validierungsziele ist die Nachverfolgbarkeit von Anforderungen an das Sollverhalten bis hin zu den Metriken, die beim Test der Systeme eingesetzt werden, unverzichtbar. Die Verbindung von Anforderungen an das im Szenarienkontext formulierte Sollverhalten zu Anforderungen an szenarioübergreifend formulierte Elemente und Schnittstellen in funktionalen, logischen und technischen Architektursichten ist somit von zentraler Bedeutung und wird beispielsweise auch durch den SOTIF-Standard (ISO 21448) - wenn auch nicht bindend - empfohlen.

Während sich in der Domäne des automatisierten Fahrens spezialisierte Methoden, Taxonomien und Terminologie entwickelt haben, stehen die neuen Herausforderungen für das Design sowie die Verifikation und Validierung automatisierter Fahrzeugsysteme bewährten Methoden des Systems Engineering gegenüber. Gerade im Hinblick auf eine konsequente Nachverfolgbarkeit von Annahmen und Anforderungen durch den gesamten Entwurfs-, Entwicklungs- und Absicherungsprozess bieten aktuelle Ansätze des modellbasierten Systems Engineering (MBSE) durch eine konsequente (semi-) formale Modellierung von Anforderungen und Systemarchitekturen potenziell hilfreiche Vorgehen für die Erstellung konsistenter Architekturbeschreibungen. Implizites Wissen über die Systeme (bestehende Architekturen, implizites Wissen über die Betriebsumgebung) kann mit entsprechenden Methoden in (semi-) formalen Modellen explizit modelliert werden. Um diese Werkzeuge effektiv und effizient einsetzen zu können, bedarf es

allerdings konsistenter Terminologie, einer Abbildung der domänenspezifischen Konzepte des automatisierten Fahrens auf die Konzepte des modellbasierten Systems Engineerings und nicht zuletzt auch Prozessen, die diese Werkzeuge anwendbar machen.

Ein Konzept das sowohl in der Domäne des automatisierten Fahrens wie auch in aktuellen Ansätzen des modellbasierten Systems Engineerings im Kontext der Systemspezifikation verwendet wird, ist das Konzept der „Fähigkeit“ [87] [88] [85] [89] als Mittel zur systematischen Ableitung von Anforderungen und Gütemaßen für (ein) System(e von Systemen) auf der Basis von Stakeholder-Bedürfnissen. Erste Ansätze zum Einsatz des Konzeptes in Prozessen zum Entwurf von Fahrzeugautomatisierungssystemen wurden z.B. von Reschka [85] und Sippl [86] beschrieben. Insgesamt ist die Einbettung der domänenspezifischen Konzepte des automatisierten Fahrens in die Terminologie und Methoden des modellbasierten Systems Engineering nach unseren Erfahrungen noch nicht ausreichend erfolgt, was sich unter anderem auch im losen Gebrauch des Begriffes in der ISO/TR 4804 niederschlägt.

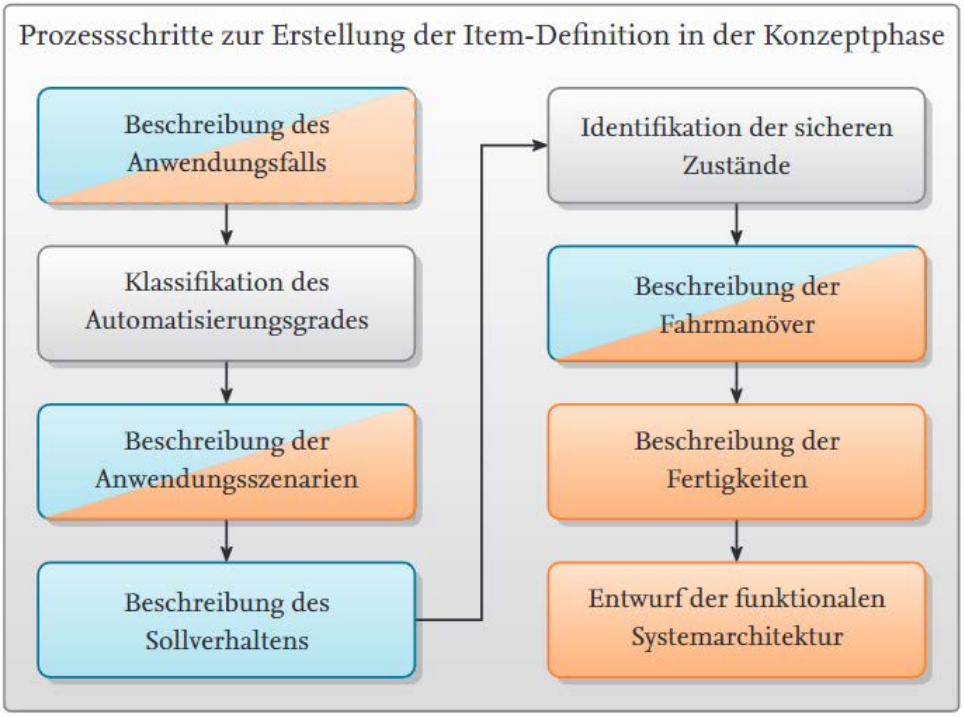


Abbildung 123: Vorgehensmodell nach Reschka: VVMethoden leistet im wesentlichen Beiträge zu den orange markierten Prozessschritten, und setzt Ergebnisse der blau markierten Prozessschritte voraus. *Hinweis:* Reschka nutzt den Begriff “Fertigkeiten”, um Konzepte zu beschreiben, die in VVM mit dem Begriff der “Fähigkeit” adressiert werden.

Aus diesem Grund wurden in VVMethoden folgende Beiträge geleistet: Es wurde eine konsistente Terminologie entwickelt, um Sollverhalten, Fähigkeiten und funktionale Architektur sowie gängige Konzepte des MBSE mit speziellen Konzepten der szenariobasierten Entwicklung automatisierter Fahrzeugsysteme zu vereinen. Auf Grundlage der harmonisierten Terminologie und der harmonisierten Konzepte wurde ein modellbasierter Ansatz zur Unterstützung der Ableitung einer funktionalen Architektur aus einer formalisierten Sollverhaltensbeschreibung für Fahrzeugautomatisierungssysteme basierend auf Reschka [85] entwickelt, dessen nicht formales Vorgehen in weiten Teilen bereits Empfehlungen erfüllt, die die ISO 21448 in nicht normativen Teilen gibt. Beiträge des verfeinerten Ansatzes sind in Abbildung 123 dargestellt.

3.1.1.8 Requirementsbreakdown zu Design und Validation / Verifikation

3.1.1.8.1 Storyline Requirement Flow

Auf der Grundlage des V-Modells definiert die Norm ISO 26262 ein Verfahren zur Gewährleistung der funktionalen Sicherheit von Systemen vor deren Inbetriebnahme. Die Abschnitte 3 (Konzeptphase) bis 7 (Produktion und Betrieb) der Norm sind an dem V-Modell ausgerichtet.

Das V-Modell wurde und wird erfolgreich für die Entwicklung von Fahrzeugen und Fahrzeugsystemen in der Automobilindustrie angewendet. Normen wie etwa die ISO 26262, ISO 21448 und Standards sowie der Stand-der-Technik beschrieben Anforderungen an die Ausgestaltung. Er ist Teil des Qualitätsmanagements.

Die Kernidee des V-Modells ist die Beschreibung des Gesamtprozesses durch eine Folge von logischen (Sub-) Prozessen. Standards, wie etwa SPICE, schlagen Detaillierungen vor, folgen aber diesem Model des Entwicklungsprozesses. Eine Darstellungsform der VVM-Gesamtmethode ist daher das V-Modell und seiner (Kern-) Ergänzungen. (siehe Abbildung 124)

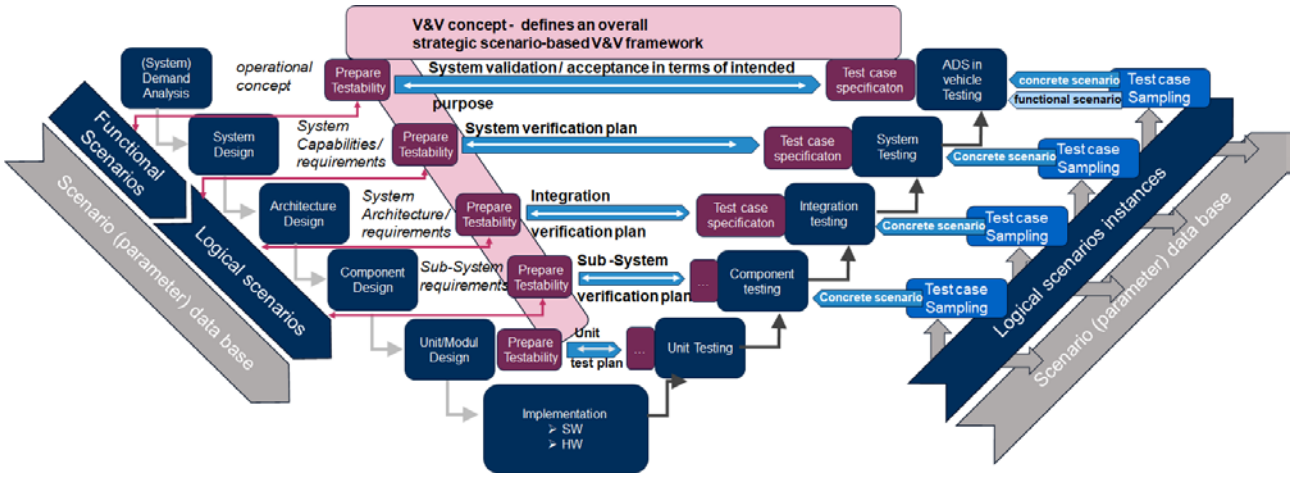


Abbildung 124: V-Modell - ergänzt um den Vorbereitungsumfänge für korrespondierende Tests

Der zentrale Kommunikationskanal in diesem Prozess-Modell sind “Requirements”. Die Bearbeitung von “Requirements” bzw. von Anforderungen ist eine wesentliche Aufgabe im Fahrzeugentwicklung. Sie ist das strukturelle Rückgrat der Normen und der Hauptkommunikationskanal für die an der Entwicklung beteiligten technische Experten. Requirements helfen bei der Zuordnung von Informationen zu verschiedenen Ebenen wie System und Architektur, Subsystem/Komponente oder Software-Unit als auch verschiedenen Komponenten . Im Zusammenhang mit der Definition von Requirements ist auch ihre “Testbarkeit” vorzubereiten. (siehe auch Abbildung 97 und Kapitel 3.1.1.9)

Der “linke Teil des V” - oft auch als der Design-Pfad bezeichnet - beginnt mit einem Betriebskonzept, das sich aus den entwicklungsrelevanten Anforderungen aus Kunden- bzw. Stakeholdersicht ableitet. Es fließt eine ODD-Analyse ein, zu der im Rahmen der VVM-Methode u.a. die Kritikalitätsanalyse (Kapitel 3.1.1.6), sowie der Rechts- und Zulassungsrahmen (Kapitel 3.1.1.3.6), Top Goals (Kapitel 3.1.1.3.8) beitragen (siehe auch Abbildung 28) und in Systemanforderungen transferiert werden. Diese werden dann zur Systemspezifikation verfeinert. Diese Besteht u.a. aus eine Sollverhaltensdefinition (Kapitel 3.1.1.7) und Systemarchitekturen auf unterschiedlichen Detailierungslevel (funktional, logisch, technisch, siehe Kapitel 3.1.1.8 in den

weiteren Abschnitten), die auch Anforderungen aus anderen Quellen beinhalten und die Definition von Abnahmekriterien erfordern.

Der nächste Schritt ist der Entwurf einer technischen Lösung mit definierten Komponenten und Schnittstellen. Diese Komponenten werden einschließlich der Akzeptanzkriterien spezifiziert. Sie werden unabhängig voneinander (dekomponiert und) entwickelt. Gegebebenfalls wird eine komplexe Komponente, wie z.B. Software, wiederum wie ein Subsystem behandelt, das einen eigenen Architekturentwurf benötigt. Bei großen Systemen kann diese Logik mehrfach angewendet werden. Die letzte Stufe dieser Systemdekomposition ist das kleinste System mit Software, Hardware und andere Technologien wie Mechanik. Der Detaillierungsgrad wie auch als auch die Anzahl der Anforderungen nimmt mit jeder Stufe zu.

Die “rechte Hälfte des V” steht für die Aktivitäten, die für die Verifizierung und Validierung erforderlich sind. Sie wird im Allgemeinen auch als "V&V Strang“ bezeichnet. In Abhängigkeit von der Integrationsstrategie gibt es unterschiedliche Integrationsschritte mit Tests, die entweder die Interfaces und Kommunikation oder die implementierte Funktion überprüfen. Den Abschluss bildet die Validierung des Gesamtsystems, bevor es eine Produktionsfreigabe erhält. (Kapitel 3.1.1.2 und 3.1.1.9)

Die Requirements müssen “testbar” sein. Dazu gehören u.a. die folgenden Anforderungen an ihre Spezifikation:

Gewisse formale Testbarkeitsanforderungen, die notwendig sind, um Testspezifikationen daraus ableiten zu können, wie etwa:

> Zuordnung von (CORE) Szenarien, in denen das Requirement gültig ist; Ausgangssituation, Eingangsdaten und Konfigurationen, Testabbruch- und Testende-Kriterium bzgl. Requirement-Verifikation; eine Güte (Evaluierungsmetrik, Referenzwert für Bestehen), Zuordnung zu Testobjekt und Testebene, Kategorie Testziel, …

Erfüllung gewisse sprachlicher Kriterien wie:

> granular, präzise, widerspruchsfrei, redundanzfrei, strukturiert formuliert, kategorisiert z.B. in Form von Testzielen hier: beispielhaft Funktion, Performance, FUSA, Zertifizierung, Komponente … (siehe z.B. Abbildung 124)

Erfüllung gewisse Vollständigkeitskriterien wie:

> der Geltungsbereich in Form von CORE Szenarien ist zu spezifizieren, Prüfkriterium, Akzeptanzkriterium für funktionale, nicht-funktionale Anforderungen, Performanz und Schnittstellenspezifikationen.

Erfüllung gewisse Tracability-Kriterien wie:

> Eine besondere prozessuale Anforderung an die Definition der Requirements ist ihre bidirektionale Rückverfolgbarkeit. Bidirektionale Rückverfolgbarkeit bedeutet, dass man in der Lage sein muss, alle abgeleiteten Requirements und alle zugehörigen Tests für jedes Requirement von jeder Ebene des Anforderungsmanagements zu finden. Außerdem muss die Rückverfolgbarkeit zwischen Anforderungen und Architekturentwurf auf System- und Softwareebene hergestellt werden, um zu zeigen, welche Komponenten welche Anforderungen erfüllen. Umgekehrt können Anforderungen an Komponenten auch aus

Architekturentwürfen abgeleitet werden. Bidirektional bedeutet auch, auf der darüber liegende Anforderungsebene das (Ausgangs-) Requirements zu finden, bis die primären Requirenments erreicht sind. Auch die Rückführung vom Software-Unit-Testfall zu den jeweiligen primären Anforderungen des Kunden muss sichergestellt sein. Aufgrund der beidseitigen Traceability ergibt sich die Implementierung eines Anforderungsmanagement-Tools. Zu den primären Anforderungen gehören rechtliche, normative, gesellschaftliche und ethische sowie herstellerbezogene Entwicklungsvorgaben (siehe auch Kapitel 3.1.1.3.8, 3.1.1.2.8 und Abbildung 28)

Diese Anforderungen bilden einen Beitrag zur Vermeidung/Reduktion des Spezifizierungsgaps sowie des Implementierungsgaps.

Aus den Requirements werden Lastenhefte abgeleitet. Diese dekomponieren das Gesamtsystem in “Komponenten” und sind Grundlage der Projektarbeit zwischen Hersteller und Zulieferern.

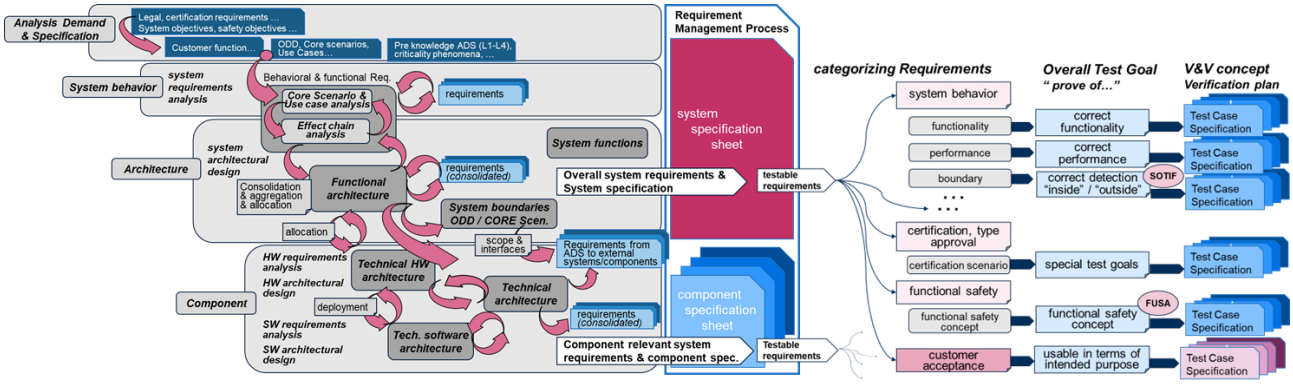


Abbildung 125: Fluss der Requirements von der Anforderungsanalyse bis zur Testfall-Spezifikation

Funktionale Sicherheit

Für das Funktionales Sicherheitskonzept werden für jedes Safety Goal / also die (funktionalen) Sicherheitsziele die „functional safety requirements“ also die funktionalen Sicherheitsanforderungen auf Testbarkeit geprüft und Testfälle abgeleitet. Die Erstellung der Testspezifikationen erfolgt auf der Grundlage der Sicherheitsanforderungen mit dem Schwerpunkt auf dem Gesamtsystem.

Die erstellten Testfälle sind mit dem zugehörigen Sicherheitsziel verknüpft. Die Sicherheitsziele werden als Anforderungen mit dem zugehörigen ASIL-Level spezifiziert und mit dem Attribut "sicherheitsrelevant" in den abgeleiteten Testspezifikationen vergeben. Sie werden auf den Teststufen der Integrationstests, Systemtests sowie im Rahmen von Fahrzeugtests mit dem integrierten ADS geprüft. Die Tests auf Systemebene (integrierte Systemkomponenten) werden für jedes Sicherheitsziel abgeleitet, soweit sie im integrierten System technisch machbar sind.

Das Technische Sicherheitskonzept beschreibt das detaillierte Sicherheitskonzept, das die Umsetzung der Lösung auf Komponentenebene und im Rahmen der Softwareentwicklung. Es wird auf den entsprechenden Komponentenebenen getestet. (siehe Abbildung 127)

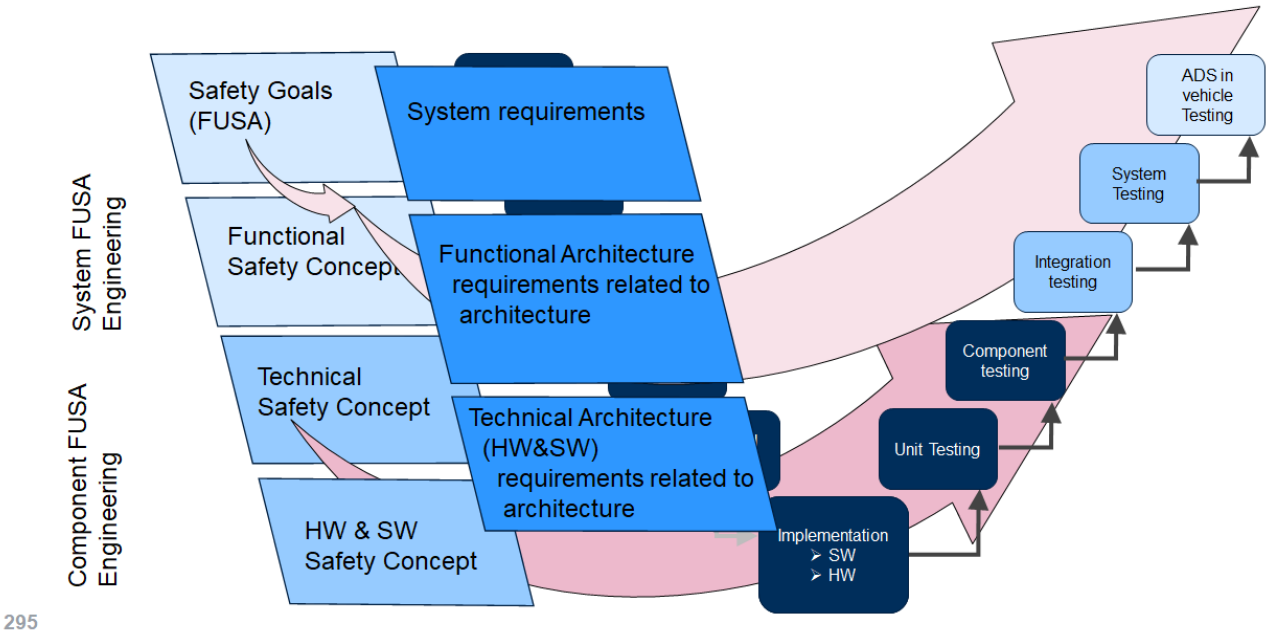


Abbildung 126: Requirement Flow zur Verifikation des Sicherheitskonzepts

Produkthaftung

Im Rahmen des Produkthaftungsgesetzes – ProdHaftG [90] gilt:

§ 1 Haftung

(1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. (…)

§ 4 Hersteller

(1) Hersteller im Sinne dieses Gesetzes ist, wer das Endprodukt, einen Grundstoff oder ein Teilprodukt hergestellt hat. Als Hersteller gilt auch jeder, der sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt.

(2) Als Hersteller gilt ferner, wer ein Produkt zum Zweck des Verkaufs, der Vermietung, des Mietkaufs oder einer anderen Form des Vertriebs mit wirtschaftlichem Zweck im Rahmen seiner geschäftlichen Tätigkeit in den Geltungsbereich des Abkommens über den Europäischen Wirtschaftsraum einführt oder verbringt.

Aus der Herstellerhaftung (§1 und §4 ProdHaftG) resultiert, dass die Validierung, die Evaluierung des Restrisikos sowie die Verifikation des integrierten Gesamtsystems bzw. des in ein Fahrzeug integrierten ADS vom Hersteller des Produktes durchgeführt werden. In Abhängigkeit von der Entwicklungstiefe des Herstellers wird die Entwicklung und Verifikation von Komponenten oder Subkomponenten von Zulieferern geleistet. Das V&V Konzept (Kapitel 3.1.1.9) beschreibt die Dekomposition der Verifizierung im Rahmen des Entwicklungsprozesses. Vor diesem Hintergrund kristallisiert sich die Relevanz der Requirements im Entwicklungsprozess sowie die Ihrer Erstellung und ihrer prozessualen Integration bzw. des Requirements-Managements heraus.

3.1.1.8.2 Requirements for Test Planning

Systemanforderungen

Systemanforderungen basieren auf den Stakeholder Needs und den Verhaltensanforderungen.

- Stakeholder Needs werden aus verschiedenen Quellen gesammelt, wie z.B. funktionalen Use Cases, einer Item-Definition oder den Kundenfunktionen.
- Verhaltensanforderungen spezifizieren die Anforderungen der Stakeholder bezüglich des Verhaltens in einem szenariospezifischen Kontexts.

Viele Anforderungen an das automatisierte Fahren sind von Sicherheitsbedenken getrieben.

- Sicherheitsziele (engl. Safety Goals, SGs) sind übergeordnete Sicherheitsanforderungen, die sich aus der Gefährdungsanalyse und Risikobewertung auf Fahrzeugebene ergeben.
- Verhaltensbezogene Sicherheitsanforderungen (Behavioral safety requirements, BSRs) spezifizieren lösungsunabhängiges sicherheitsrelevantes Verhalten oder lösungsunabhängige Sicherheitsmaßnahmen einschließlich ihrer sicherheitsrelevanten Attribute.

Die Anwendung der Goal/Question/Metric (GQM) Methode auf ausgewählte funktionale Anforderungen liefert uns Gütemaße. Diese werden als Performance-Anforderungen formuliert, welche die funktionalen Anforderungen ergänzen.

- Funktionale Anforderungen sind Aussagen, die identifizieren, welche Ergebnisse ein Produkt oder Prozess erzielen soll.
- Performance Anforderungen sind messbare Kriterien, die identifizieren, wie gut funktionale Anforderungen erfüllt werden sollen

Funktionale Architektur

Eine funktionale Architektur erfüllt die Systemanforderungen, indem sie ausreichende Funktionalität definiert. Während der Ausarbeitung der funktionalen Architektur werden die Systemanforderungen parallel verfeinert.

VVM-Glossar “Funktionale Architektur”:

> „Hierarchische Anordnung von Funktionen, ihren internen und externen funktionalen Schnittstellen und externen physischen Schnittstellen, ihren jeweiligen funktionalen und Performance Anforderungen sowie ihrer Designbeschränkungen.“

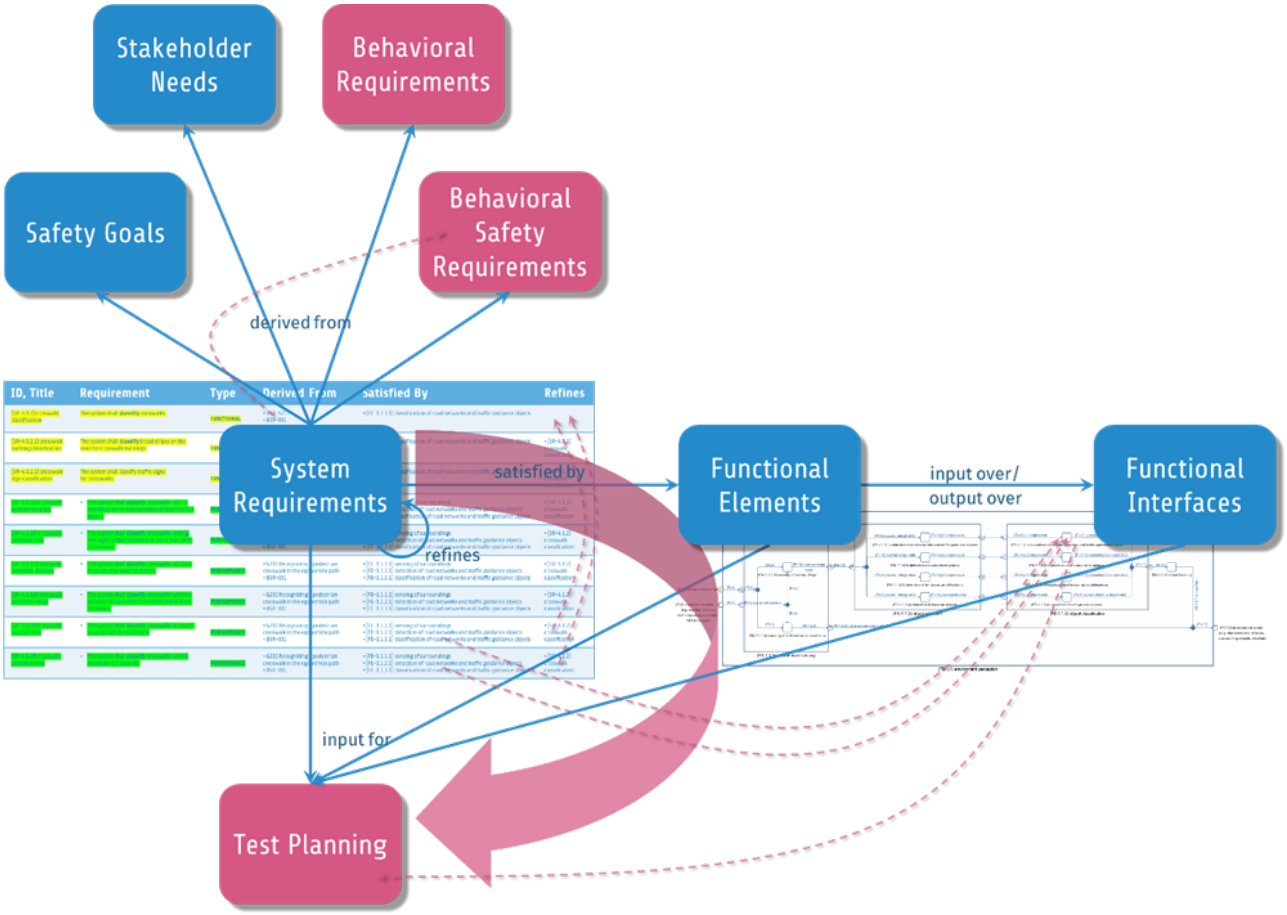


Abbildung 127: Anforderungsmanagement und Anforderungs-Flow zur Test-Planung

Übergabe zur Testplanung

Die funktionalen Elemente der funktionalen Architektur werden als Testobjekte an die Testplanung übergeben. Die funktionalen Elemente bündeln ihre zugehörigen Systemanforderungen. Die enthaltenen Performance-Anforderungen sind Ziele bei der Festlegung von Bestehen/Nicht-Bestehen-Kriterien für Tests.

3.1.1.8.3 Requirements for Test Orchestration

Systemanforderungen

Systemanforderungen basieren auf den Stakeholder Needs und den Verhaltensanforderungen.

Sicherheitsziele und verhaltensbezogene Sicherheitsanforderungen (engl. Behavioral Safety Requirements, BSRs) reichern diese mit Sicherheitsaspekten an.

Eine **funktionale Architektur** erfüllt die Systemanforderungen.

Logische Architektur

Eine logische Architektur gruppiert Funktionen und berücksichtigt nicht-funktionale Anforderungen unter Verwendung technischer Konzepte und Prinzipien.

Das Vorhandensein einer logischen Architektur mildert die Auswirkungen von Anforderungs- und Technologieänderungen auf das Systemdesign.

Eine **technische Architektur** implementiert logische Elemente und ihre Schnittstellen durch spezifische Technologie.

Übergabe zur Test-Orchestrierung

Die technischen Elemente der technischen Architektur werden als Testobjekte an die Test-Orchestrierung übergeben. Technische Elemente bündeln ihre zugehörigen Anforderungen an technische Elemente, die verifiziert werden müssen.

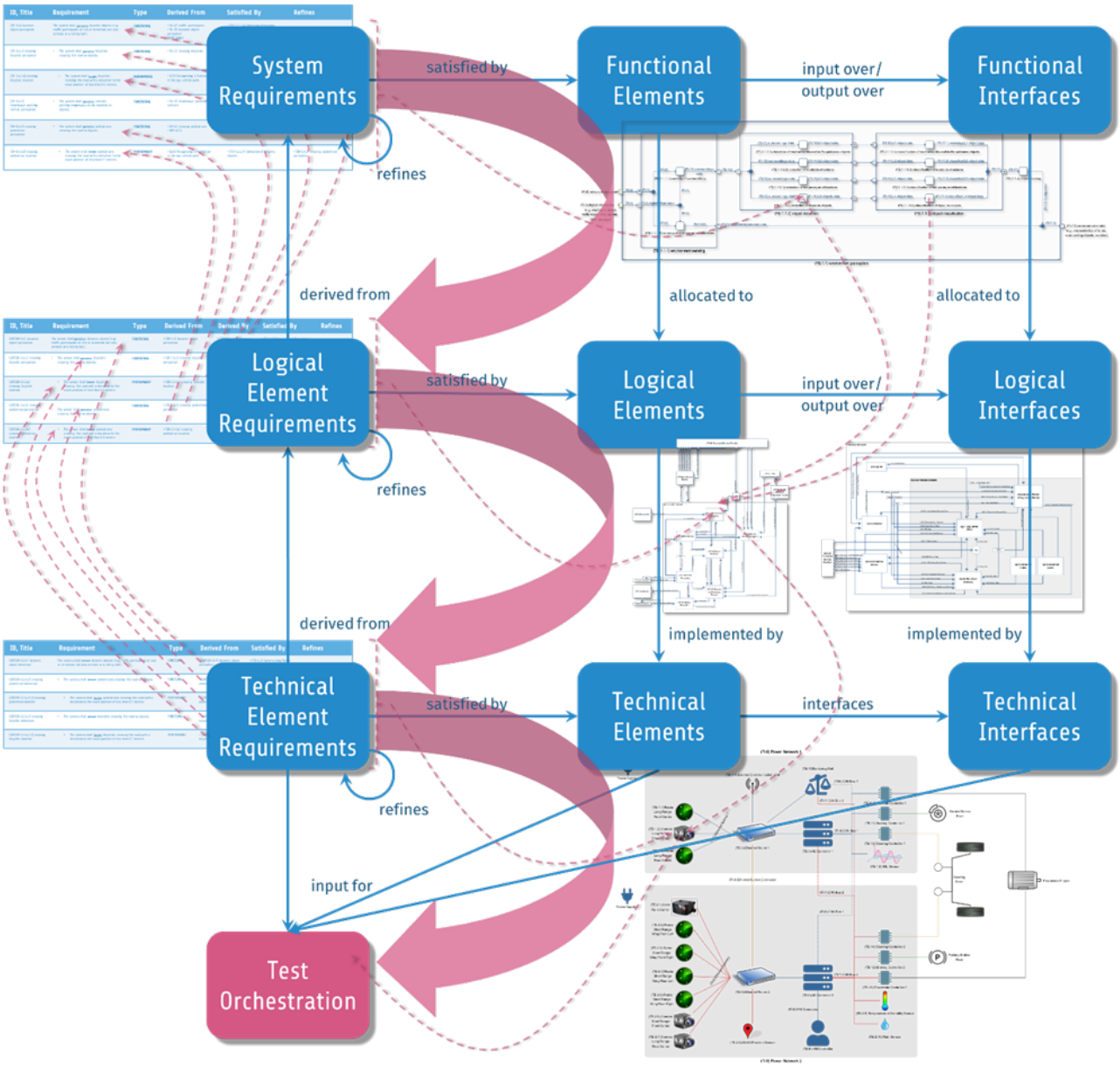


Abbildung 128 Anforderungs-Flow zur Test-Orchestrierung

3.1.1.8.4 Safety-related Quality Measures: From Risk Reduction Need to Design Constraints

Gütemaße für Sicherheitsziele

Der in VVM entwickelte Risk Management Core leitet die primären Gütemaße für die Sicherheit ab: Risikominderungsbedarf und Integrität (engl. risk reduction need and integrity). Diese Maße

werden den übergeordneten Sicherheitsanforderungen zugeordnet, den Sicherheitszielen (engl. Safety Goals).

Gütemaße für Verhaltensbezogene Sicherheitsanforderungen

Die Beschreibung von Sollverhalten beinhaltet die Definition von Sicherheitsmaßnahmen (engl. Safety Measures) im Rahmen eines Verhaltensbezogenen Sicherheitskonzepts (engl. Behavioral Safety Concept). Diese Sicherheitsmaßnahmen werden durch Verhaltensbezogene Sicherheitsanforderungen (engl. Behavioral Safety Requirements) formuliert.
Im Zuge der Sollverhaltensspezifikation erhalten die Verhaltensbezogenen Sicherheits-anforderungen Gütemaße für die Sicherheit: Risikominderungsbedarf und Integrität (engl. risk reduction need and integrity).

Gütemaße für Funktionale Sicherheitsanforderungen

Funktionale Sicherheitsanforderungen bilden das Funktionale Sicherheitskonzept. Im Projekt VVM werden Gütemaße für Funktionale Sicherheitsanforderungen als Performance Anforderungen (engl. performance requirements) bezeichnet.
Diese Performance Anforderungen repräsentieren die Erfüllungskriterien der Funktionalen Sicherheitsanforderungen. Sie stellen Design-Einschränkungen (engl. design constraints) für das System Design dar.

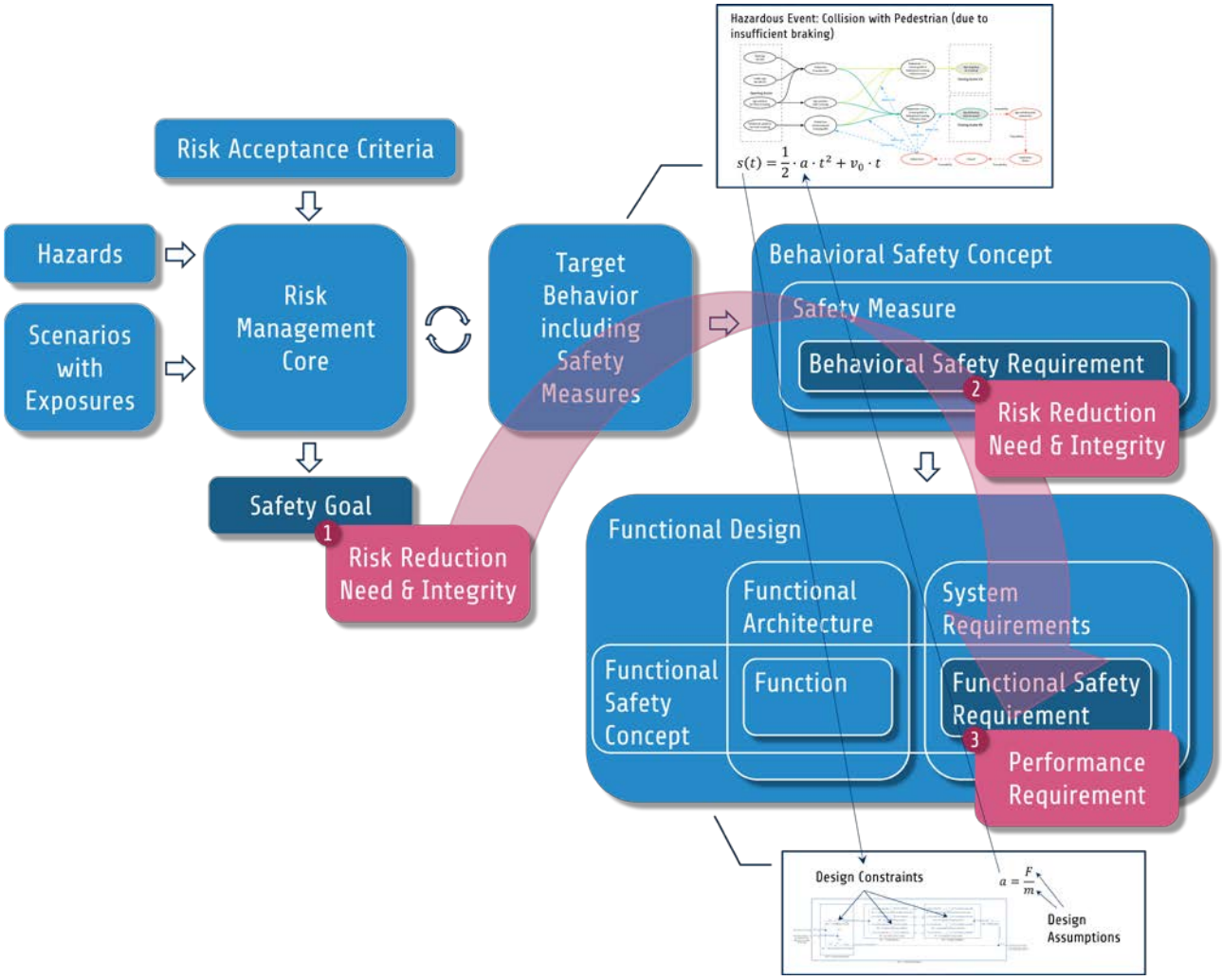


Abbildung 129 Kette der Gütemaße mit Sicherheitsbezug

Herausforderung: Gütemaße für Verhaltensbezogene Sicherheitsanforderungen und Funktionale Sicherheitsanforderungen in Einklang bringen

- Qualitätsmaße für Verhaltensbezogene Sicherheitsanforderungen werden auf Basis von Risiken formuliert.
- Performance Anforderungen als Qualitätsmaße für Funktionale Sicherheitsanforderungen werden auf Basis von technischen Werten (z.B. physikalische Größen wie Entfernungen) formuliert.

Um diese beiden Arten von Qualitätsmaßen in Einklang zu bringen, muss die Leistungsfähigkeit des Systems mit einem Szenario-basierten Ansatz bewertet werden. Diese Bewertung kann dann auf der Verhaltensebene zur Abschätzung des Restrisikos dienen.

3.1.1.8.5 Examples for Quality Measures

Dieses Beispiel zeigt das Verhältnis der Gütemaße von Verhaltensbezogenen Sicherheitsanforderungen und Funktionalen Sicherheitsanforderungen.

Sicherheitsziel: Verhindere die Kollision eines Straßenfahrzeuges mit einem x am Fußgängerüberweg.

Verhaltensbezogene Sicherheitsanforderung: Ein Straßenfahrzeug muss in der Lage sein die Querungsabsicht eines Fußgängers zu erkennen, um die Querungsabsicht von Fußgängern beim Treffen von Fahrentscheidungen zu berücksichtigen.

- Nominale Risikominderung: 1234 x 10^{-10} Todesfälle beim Überqueren pro Betriebsstunde
- Integrität: 100 x 10^{-10} Todesfälle beim Überqueren pro Betriebsstunde

Einschränkungen

- Die erlaubte Höchstgeschwindigkeit für Fahrzeuge beträgt 30 km/h (Spezifizierung VVM Functional Use Case 2 „Straight Passing of a T-Crossing with Pedestrian Crossing“).
- Bei einer erlaubten Höchstgeschwindigkeit von 30 km/h muss in Deutschland ein Fußgängerüberweg in mindestens 50 Metern Entfernung sichtbar sein [91].
- Bei einer erlaubten Höchstgeschwindigkeit von 30 km/h muss in Deutschland die Wartefläche eines Fußgängerüberwegs in mindestens 30 Metern Entfernung sichtbar sein [91].

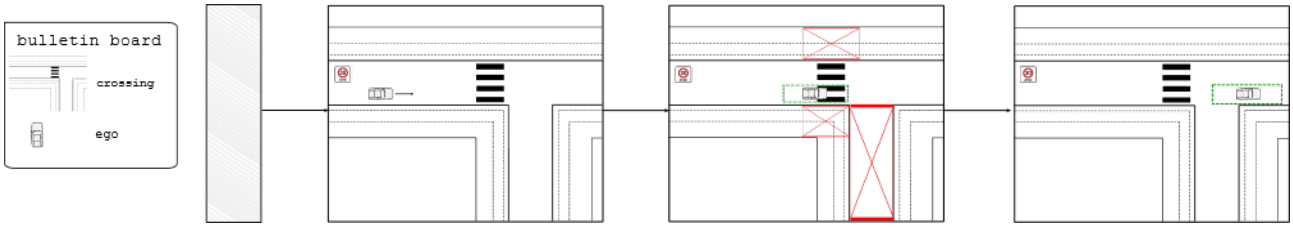


Abbildung 130: VVM Functional Use Case "FUC2 – Straight Passing of a T-Crossing with Pedestrian Crossing“

Funktionale Sicherheitsanforderungen

ID, Title	Type	Requirement
(SR-4.1.2) crosswalk classification	Functional	The system shall classify crosswalks.
(SR-4.1.2a) crosswalk position accuracy	Performance	The system shall classify crosswalks with a deviation to the exact position of less than 0.3 meters.
(SR-4.1.2b) crosswalk detection rate	Performance	The system shall classify crosswalks during free sight within 50 meters in more than 99% of the cases.
(SR-4.1.2c) crosswalk detection distance	Performance	The system shall classify crosswalks within a distance of at least 50 meters.
(SR-4.1.2d) crosswalk detection range	Performance	The system shall classify crosswalks within a distance of more than 0.3 meters and at least 50 meters.
(SR-4.1.2e) crosswalk reaction time	Performance	The system shall classify crosswalks at least 5 seconds before reaching it.
(SR-4.1.2f) crosswalk detection time	Performance	The system shall classify crosswalks within maximum 0.5 seconds.

Abbildung 131 Systemanforderungen in der Nähe von Fußgängerübergängen in Bezug auf Safety

Erkennung eines Fußgängerüberwegs

Anforderung zur Erreichung der nominalen Leistung

- Die Erkennung eines Fußgängerüberwegs darf höchstens 0,5 Sekunden benötigen (SR-4.1.2f).

- 0,5 Sekunden bei einer Geschwindigkeit von 30 km/h entsprechen einer zurückgelegten Strecke von 4,2 Metern.

Anforderungen zur Erreichung der Integrität

- Ein Fußgängerüberweg soll mit einer maximalen Abweichung von 0,3 Metern erkannt werden (SR-4.1.2a).
- Die Geschwindigkeit unseres Fahrzeuges soll mit einer maximalen Abweichung von 5 Prozent ermittelt werden (SR-2.1a).
  - 5 Prozent Abweichung von 30 km/h entsprechen einer Abweichung von 1,5 km/h.
  - 0,5 Sekunden zur Erkennung eines Fußgängerüberwegs bei einer um 1,5 km/h höheren Geschwindigkeit entspricht einer zusätzlich zurückgelegten Strecke von 0,2 Metern.

Reaktion auf einen Fußgängerüberweg

Anforderung zur Erreichung der nominalen Leistung:

- Nach der Erkennung eines Fußgängerüberwegs muss dieser noch mindestens 5 Sekunden entfernt sein (SR-4.1.2e).
  - 5 Sekunden bei einer Geschwindigkeit von 30 km/h entsprechen einer Entfernung von 41,7 Metern.

Anforderungen zur Erreichung der Integrität

- Die Geschwindigkeit unseres Fahrzeuges soll mit einer maximalen Abweichung von 5 Prozent ermittelt werden (SR-2.1a).
  - 5 Prozent Abweichung von 30 km/h entsprechen einer Abweichung von 1,5 km/h.
  - 5 Sekunden Entfernung zum Fußgängerüberweg bei einer um 1,5 km/h höheren Geschwindigkeit entspricht einer zusätzlich zurückgelegten Strecke von 2,1 Metern.

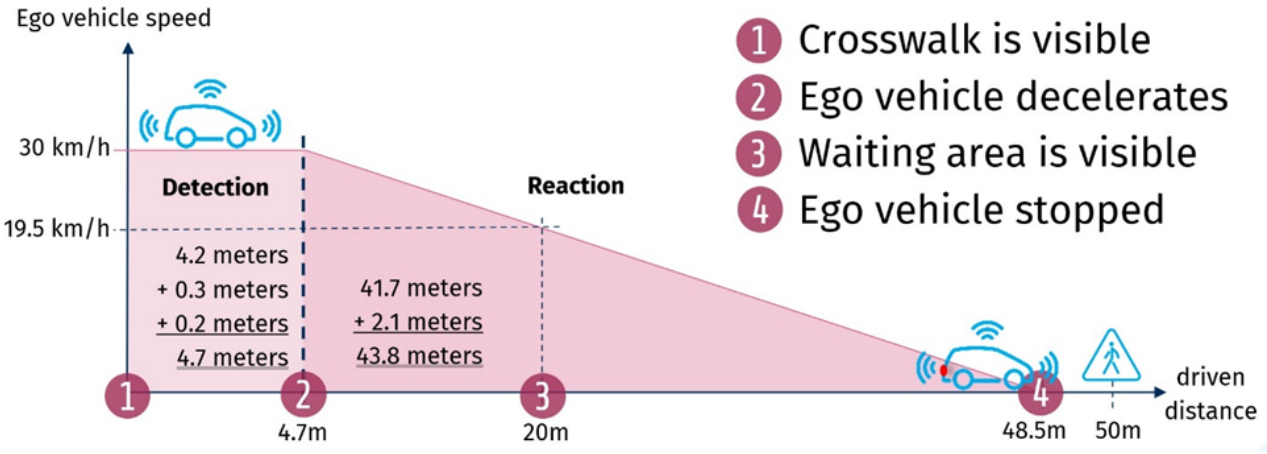


Abbildung 132: Fahrzeug verlangsamt, wenn es sich einem Fußgängerüberweg mit Fußgänger nähert

3.1.1.9 V&V-Domäne

3.1.1.9.1 V&V Domäne - Überblick

V&V innerhalb des Assurance Frameworks und seiner Schnittstellen

Das Ziel von V&V ist es, durch die Bereitstellung von ausgewerteten Testergebnissen zu einer ganzheitlichen Aussage über die Sicherheit beizutragen. Als integraler Bestandteil des Assurance Frameworks ist V&V auf Eingaben zu Sicherheitsfähigkeiten, Anforderungen an das V&V-Konzept und Informationen zum Systementwurf angewiesen.

Angepasst an den zweistufigen Ansatz bei der Entwicklung des funktionalen (lösungsunabhängigen) und technischen (technologischen) Entwurfs wird auch die Bearbeitung der Tests in einen funktionalen und einen technischen Schritt unterteilt.

Darüber hinaus werden logische Szenario-Instanzen benötigt, die aus dem jeweiligen Prozess in die Testplanung einfließen.

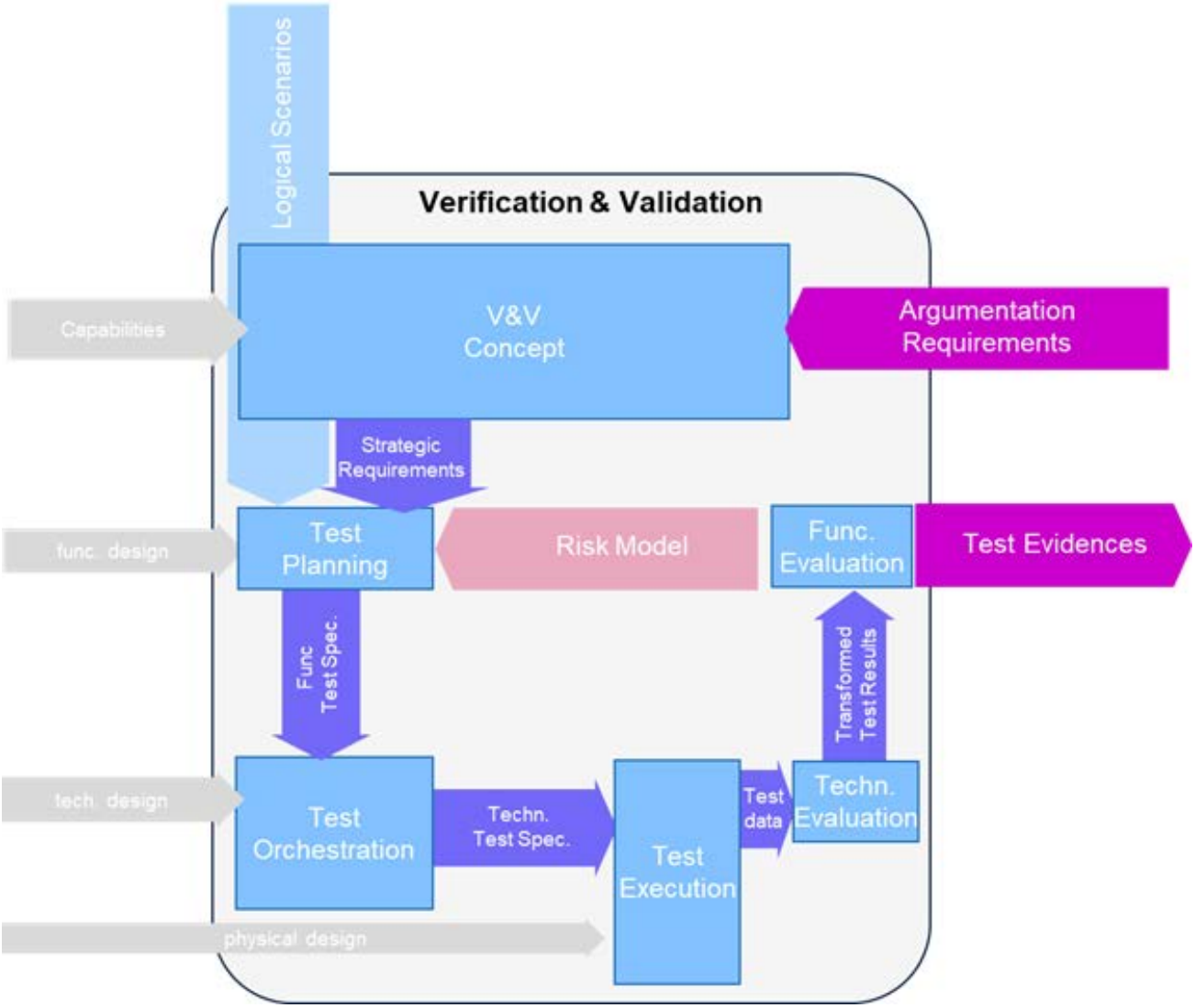


Abbildung 133: The structure of V&V within the Assurance Framework

Verbindung zur Argumentation

Eine Sicherheitsargumentation erfordert zwei Hauptaspekte aus dem Bereich V&V:

- Konzepte, auf denen die Argumentation eine Strategie aufbauen kann,
- geeignete Evidenzen

Beide Inputs müssen den Regeln und der Systematik der Argumentation folgen.

Evaluierung des Risikos

Das Risikomanagement benötigt Nachweise für die Bewertung der spezifizierten Risikominderung der Maßnahmen der Sicherheitskonzepte. Die Aspekte der Nachweise müssen den Anforderungen der definierten Risikomodellierung und insbesondere den Akzeptanzkriterien folgen. Dies unterstützt die Übertragung der Risikomodellierung auf das technische System. Aus der Erfüllung einer definierten Risikominderung können Testendekriterien abgeleitet werden.

Prozessablauf innerhalb V&V

V&V-Konzept - Das V&V-Konzept beschreibt die Vorgehensweise bei der Erbringung der für die Argumentation benötigten Evidenzen Hierbei wird die Erfassung systematisiert.

Testplanung - Definition des funktionalen Testraums und Erstellen der funktionalen Testspezifikationen.

Test Orchestration - Ableitung von technischen Testspezifikationen aus funktionalen Testspezifikationen unter Verwendung von Wissen über den technischen Entwurf und die Testplattformen. Verteilen von Testfällen auf Testinstanzen.

Testdurchführung - Durchführen von Tests gemäß den technischen Testspezifikationen.

Technische Auswertung - Technische Auswertung der bei der Testdurchführung erzeugten Testdaten, entsprechend der Testorchestrierung.

Funktionale Auswertung - Bewertung der Funktionen auf der Grundlage der Eingaben der technischen Auswertung, entsprechend der Testplanung. Aggregieren der Ergebnisse, um die Sicherheit des ADS zu belegen.

Behandlung von Concerns innerhalb V&V

Concerns sind Hinweise subjektiver (z.B. Einschätzungen) oder objektiver (z.B. Messergebnisse) oder normativer (z.B. Normen & Gesetze) Natur, die hinsichtlich des Umfangs der Tests besonders berücksichtigt werden müssen. Die Concerns müssen auf der entsprechenden Ebene angesprochen werden. So beziehen sich z. B. funktionale Concerns auf die funktionale Gestaltung, während Szenario-Concerns sich auf Szenarien beziehen, die berücksichtigt werden müssen. Entsprechend ihrer Ebene werden solche Concerns an der geeigneten Stelle aufgenommen, um ihre Relevanz für die Sicherheit im Kontext z.B. des funktionalen Designs oder der logischen Szenarien-Instanzen zu gewichten.

Szenario-basierte Methode für die Absicherung eines ADS (Verifikation & Validierung)

Im Rahmen der Absicherung, also der Verifikation und Validierung, des Entwicklungsstandes eines ADS wird durch Testen überprüft, ob das aktuelle Release des ADS

- spezifikationskonform (“Ist das System richtig [im Rahmen der identifizierten Anforderungen] entwickelt?”) sowie
- nutzenkonform (“Ist das richtige System [im Rahmen der gewählten Entwicklungsziele] entwickelt?”)

ist. Das gesamtmethodische Vorgehen von VVM ist in Kapitel 3.1.1.2 detailliert beschrieben.

Prozessabhängigkeiten im szenariobasierten Entwurf einschließlich V&V.

- Das ODD-Metamodell wird (neu) im bestehenden Entwicklungs- und Validierungsprozess durchgängig als valides Modell der (Ziel) ODD benutzt und im Rahmen der ADS Validierung (neu, zusätzlich) auf Abgeschlossenheit überprüft. Daraus ergibt sich
    - einerseits die neue Aufgabe im Rahmen der Validierung, die ausreichende Güte des aktuellen Satzes von CORE-Szenarien zu überprüfen. D.h. es muss nachgewiesen werden, dass der Satz von CORE-Szenarien und die instanziierten Eigenschaften die realen Szenarien, die in der Zieldomäne vorkommen, ausreichend abdecken. (Abbildung 134)
    - andererseits muss eine Risikoanalyse im Rahmen des Systemdesigns (rechte Seite V-Modell) durchgeführt wurden.
- Die Evaluierung des (im Rahmen des Systementwurfs) risikokontrollierten (Sicherheits-) Verhaltens des Systems wird (neu) hinzugefügt, wobei es von entscheidender Bedeutung ist, dass sich das System sicher verhält oder dass die Kriterien für die Risikoakzeptanz in seiner ODD erfüllt sind.
- Das V&V Konzept fokussiert (neu) auf einer “Safety assurance” orientierten Gestaltung, die argumentations-zentriert ausgerichtet ist. Aus diesem Grund werden die Testobjekte, die Testziele, die Testebenen, die Testplattformen und die Teststrategien durch das V&V-Konzept miteinander verknüpft und auf den Bedarf an Artefakten und Nachweisen für den Aufbau des Sicherheitsarguments ausgerichtet.

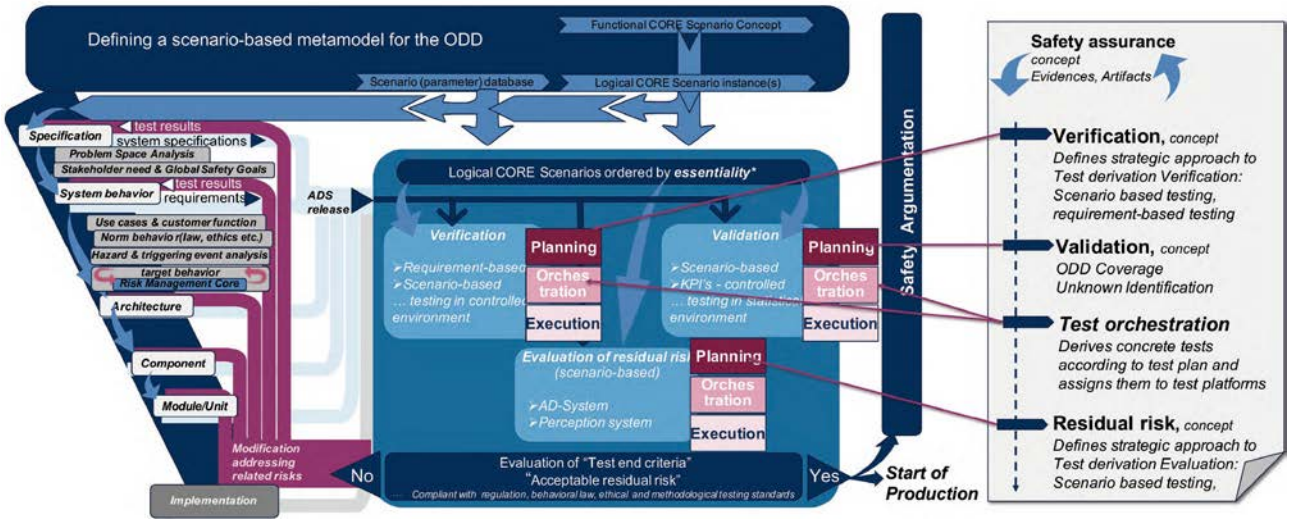


Abbildung 134: Prozess-Sicht V&V im Rahmen einer scenariobasierten VVM Gesamtmethode

Das V&V-Konzept gibt einen Überblick über die wichtigsten strategischen Bereiche, die für alle Aspekte der Verifizierung und Validierung (V&V) gelten. Dazu gehören eine gemeinsame Denkweise, die allgemeinen Ziele der V&V, ihre gegenseitigen Abhängigkeiten und Wechselwirkungen sowie die KPIs. Das Verifikationskonzept und das Validierungskonzept sind grundlegende Elemente des V&V-Konzepts. Es wird ein Freigabekriterium für die Produktion festgelegt. Dieses definiert das Ende der V&V-Aktivität. Ein wesentlicher Bestandteil ist die “Evaluierung des Restrisikos” auf dem ODD-Metamodell. Darüber hinaus enthält es eine Zusammenfassung der Organisation und der Rollen, die in der Organisation enthalten sind.

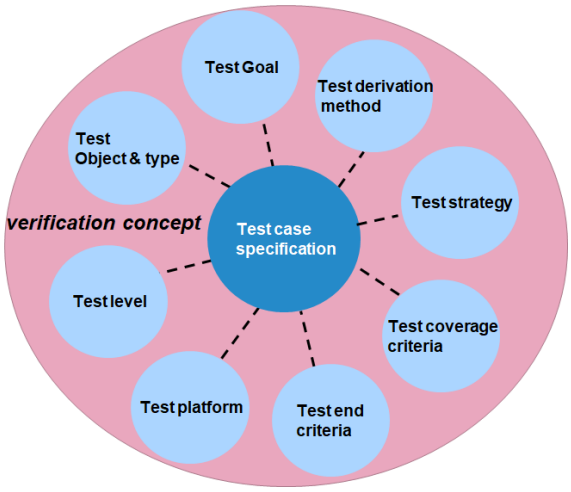


Abbildung 135: Test-Konzept

Das Verifikationskonzept beschreibt die Methoden, um die Systemfunktionalität zu verifizieren und um zu zeigen, dass alle Anforderungen in der richtigen Weise umgesetzt wurden ("das Produkt wurde richtig entwickelt"). Das Verifikationskonzept enthält einen Überblick über das System, seine Architektur und seine Funktionalität. Es definiert, was getestet wird (Testziele), für welche Zwecke der Test die Erfüllung nachweisen soll (Testziele) und auf welchen Ebenen die verschiedenen Systemelemente getestet werden (Teststufen). Es enthält allgemeine Teststrategien, die verwendeten Testumgebungen (Testplattformen) und eine Testmatrix mit einer detaillierten Zuordnung, die durchgeführten Tests mit den Systemanforderungen verbindet (Abbildung 135). Darüber hinaus werden die Normen ISO 26262 und 21448 berücksichtigt.

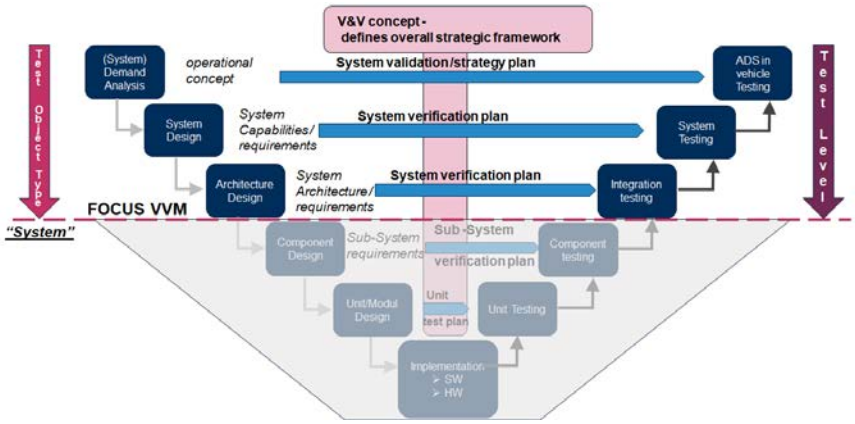


Abbildung 136: Fokus VVM “Systemebene”

Abbildung 136 zeigt den Fokus von VVM in der V&V Domäne auf die Systemebene. Dies trägt dem besseren Verständnis bei. Alles hier Dargestellte lässt aber leicht auch auf tiefere Ebenen übertragen.

Das Validierungskonzept beschreibt alle Methoden, Prozesse und Arbeitsprodukte, die erforderlich sind, um durch objektive Nachweise zu bestätigen, dass das entwickelte System tatsächlich seinen beabsichtigten Zweck erfüllt und den Nutzeranforderungen entspricht, für die es entwickelt wurde. Ziel der Validierung ist es, den Nachweis zu erbringen, dass die hohen Anforderungen an die Verhaltenssicherheit, Leistungsfähigkeit und Compliance des Produktes, die sichere Bewältigung aller möglichen (Verkehrs-)Situationen, die Kundenzufriedenheit sowie die Anforderungen aus Zertifizierungen und Vorschriften erfüllt werden. Die Validierung erweitert die Verifikation in dem Sinne, dass ihr Ziel darin besteht, die unbekannten Unbekannten (ontologische Unsicherheiten) sowie unbekannte Zusammenhänge bekannter Phänomene (epistemische Unsicherheiten) zu reduzieren, das zu finden, woran im Rahmen der Entwicklung nicht gedacht wurde / was nicht explizit durch Testfälle während des Verifikationsprozesses definiert wurde. Das Validierungskonzept berücksichtigt SOTIF-Aspekte in Bezug auf ISO 21448.

Das Verifikationskonzept und das Validierungskonzept definieren die Testkonzepte für dasselbe zugrundeliegende System. Im Rahmen des VVM-Ansatzes gründet sich der Entwicklungsprozess auf der durchgängigen Verwendung des ODD Metamodells. Daher sind Testobjekte, Testziele, Testebenen, Testplattformen und Teststrategien durch das V&V-Konzept szenarienbasiert miteinander verbunden.

Die Validierungsziele zeigen, dass die Akzeptanzkriterien während des Betriebs des ADS in der ODD in einem offenen Kontext mit ausreichendem Konfidenzniveau erfüllt werden. Die Verifikationsergebnisse zeigen dementsprechend, dass die Validierungsziele für die bekannten Gefährdungsszenarien der ODD erreicht werden und dass das Restrisiko aus den bekannten Gefährdungsszenarien nicht unangemessen ist.

Szenariobasierte Verifikation

Der Zweck der szenariobasierten Verifikation in der gesamten VVM-Methodik ist es, das implementierte Verhalten anforderungsbasiert oder gegen die ADS-Spezifikation zu überprüfen. Das Verhalten wird durch szenariobasiertes Testen auf der Basis des ADS-Metamodells und der zugehörigen Parameterräume verifiziert. (Abbildung 137) Die Verifikation weist nach, dass die

spezifizierten Anforderungen an das Produkt durch objektive Nachweise (d.h. Tests und Bewertungen) erfüllt werden.

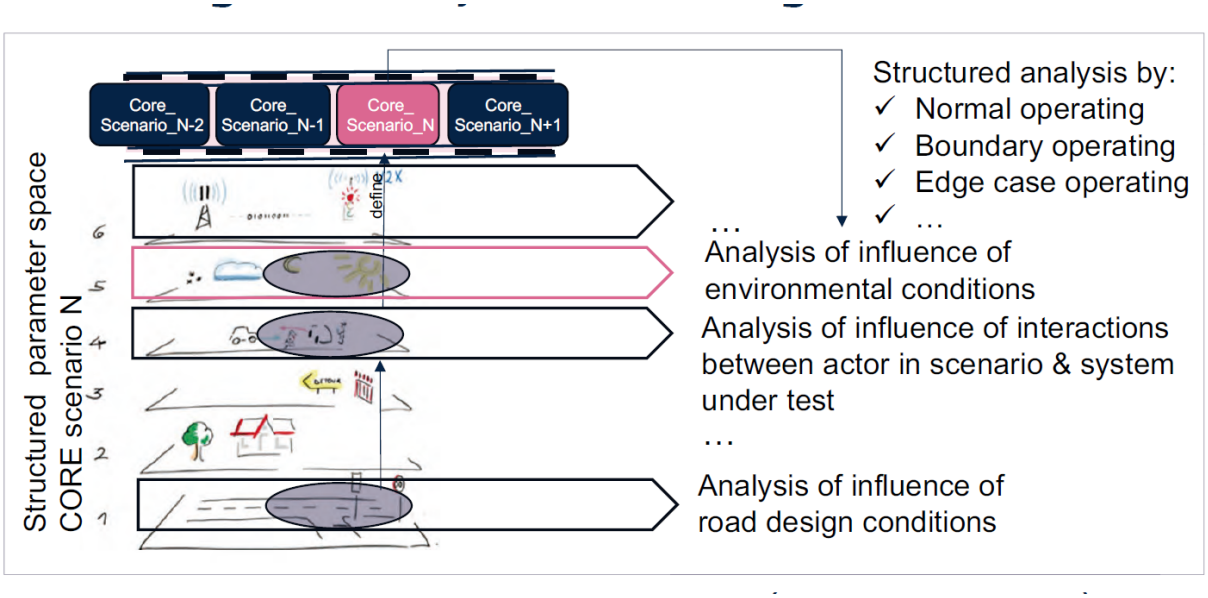


Abbildung 137: Parameter-Sampling im Rahmen des szenariobasierten Testens.

Szenariobasierte Validierung

Der Zweck der szenariobasierten Validierung in der VVM-Methodik ist die strecken- und szenariobasierte Erprobung des ADS in der realen Betriebsdomäne im Verkehr auf öffentlichen Straßen mit Hilfe von Dauerläufen oder feldbasierten Tests unter nicht-deterministischen / stochastischen Bedingungen. Zentrale Aufgaben sind das Aufdecken von "Unbekannten / Unbekannten", "unvollständigen" Spezifikationen oder Implementierungen, das Aufdecken von Triggern für "unbeabsichtigtes (unsicheres) Verhalten" sowie von nicht bestätigten Annahmen, die in den Entwicklungsprozess zum Beispiel im Rahmen der Analyse und Spezifikation eingeflossen sind. Ziel der Validierung ist der Nachweis, dass die Entwicklungsziele erreicht wurden. Das heißt, dass das richtige System entwickelt wurde. Dies umfasst die Umsetzung der Anforderungen an die Sicherheit und Leistungsfähigkeit des ADS, die sichere Bewältigung aller möglichen (Verkehrs-) Szenarien sowie die Zufriedenheit und Akzeptanz der Kundinnen und Kunden. Es wird auch zum Testen aller Eigenschaften von Szenarien verwendet, die nicht in der Simulation getestet werden können oder Szenarien, die nicht auf dem Testgelände durchgeführt werden können. Aus diesem Grund ist der Nachweis der genauen Erkennung der Grenzen der (realen) ODD und der Aktivierung des Systems nur innerhalb der ODD möglich. Dazu gehört auch, zu überprüfen ob das System die Regeln der Verkehrs- bzw. Verhaltensgesetze einhält. Darüber hinaus werden die Daten mit Hilfe von Kritikalitätsmetriken ausgewertet, die eine Bewertung der potentiellen Sicherheitsrisiken und des regelkonformen Verhaltens ermöglichen. (Abbildung 138)

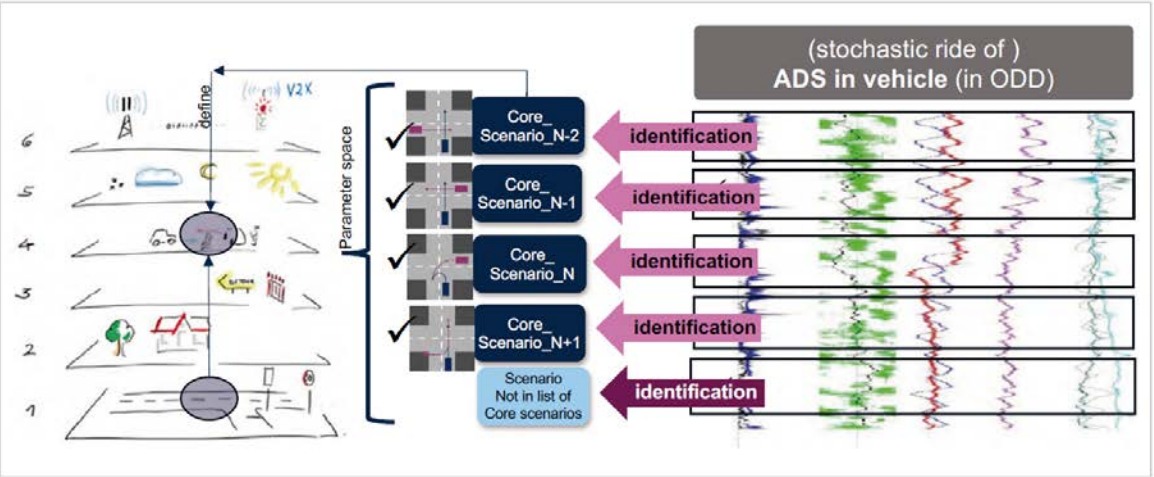


Abbildung 138: ODD-Validierung der Vollständigkeit des ODD Metamodells

3.1.1.9.2 V&V Konzept

Das V&V Konzept bildet einen wesentlichen prozessualen Bestandteil der Domäne der Verifikation und Validation in der VVM-Methode. Typischerweise werden die Inhalte des V&V Konzeptes auch als V&V-Strategie bezeichnet. Neu ist die konsequente Zuordnung zu einer abstrakten Systembetrachtung im Rahmen des Capability Layers, die systematische Aufgabe bezüglich der Evidenzerbringung für die Argumentation und die damit einhergehende Steuerung durch die Argumentation und indirekt durch das Risikomanagement. Neu ist auch die Rückwirkung auf die Designdomäne bezüglich der V&V Fähigkeiten.

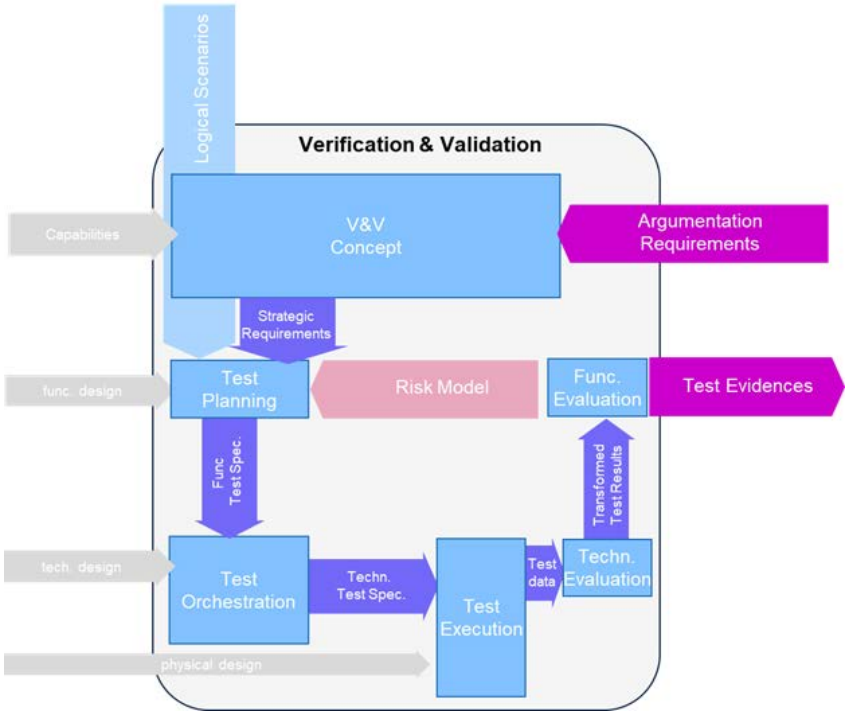


Abbildung 139: Schematische Darstellung des V&V Konzeptes

Scope des V&V Konzepts

Das V&V Konzept beschreibt das strategische Vorgehen, wie die für die Argumentation notwendigen Evidenzen durch Verifikation und Validierung erzeugt werden, also in der Systematisierung der Erfassung der Evidenzen. Es beinhaltet ein Verifikationskonzept, ein Validierungskonzept, eine Vorgehensweise zur Evaluierung des Risikos sowie Testendekriterien, die insbesondere ein Risikoakzeptanzlevel enthalten. Hierdurch können ADS-Safety-Cases begründet werden. Ziel der ADS-Safety-Cases ist dabei die Einhaltung von sicherem und konformen Sollverhaltens eines ADS nachzuweisen.

Ansatz

Es werden Testfälle für die Verifizierung und Validierung (V&V) aus der Zerlegung von System-, ODD- und TOP-Ziele-Anforderungen generiert. Diese Zerlegung erfolgt unter der Zielstellung des Nachweises der Sicherheit des Verhaltens des Systems in der ODD. Die Summe der Testfälle aus V&V auf allen Systemebenen liefert die Grundlagen für den Beweis, dass das „System-Ist-Verhalten“ das Zielverhalten in der definierten ODD darstellt und somit die TOP-Ziele z.B.: "Sicherheit durch Abwesenheit eines unangemessenen Risikos" erfüllt.

Anforderungen an die Prozesserfüllung - Beispiel

- Abdeckung der Sicherheit in Bezug auf FuSi, Sicherheit, Verhalten/SOTIF, Ethik, Einhaltung von Standards.

Anforderungen an die Methode - Beispiele

- Die Methode sollte einen Sicherheitsnachweis darstellen. Dieser Sicherheitsnachweis sollte risikobasiert ausreichend argumentiert und rückverfolgbar sowie in Übereinstimmung mit Spezifikationen und Abnahmekriterien erstellt werden.
- Die Methode sollte in Übereinstimmung mit den Argumentationsprinzipien erstellt werden.
- Die Methode sollte reelle Machbarkeit, Effizient und Änderungsfreundlichkeit beinhalten.
- Die Methode sollte Anwendungen enthalten wie z.B. Szenariobasiertes Testen, Struktur für Kennzahlen/Metriken,..

Prozess

1. Definition von Risikoschwellen entlang des Risikomodells auf Basis einer gemeinsamen Zerlegung von ODD und Designs mit dem Resultat der Festlegung von Performance-Schwellen.
2. Durchführung der Verifizierung des Systems bis zum Nachweis aller Performance-Schwellen. Sofern dies nicht gelingt, muss die Entwicklung iteriert werden.
3. Durchführung der Validierung des Systems, um zu beweisen, dass das Risiko unter den Risikoschwellen liegt. Sofern dies nicht gelingt, muss die Entwicklung iteriert werden.

Je tiefer der Verifikationsraum erfasst wird, desto weniger Aufwand wird für die Validierung benötigt.

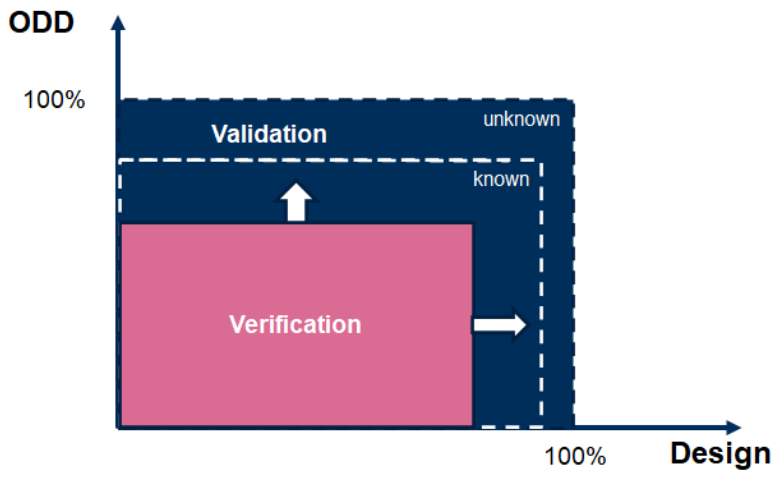


Abbildung 140: Abdeckung von V&V-Prozessen am Dekompositionsraum von ODD & Design (© VVM)

Verifikation - Objektiv: Überprüfung der Anforderungen und der korrekten Integration der Komponenten und des Gesamtsystems.

Wesentliches neues Element: Zielsetzung der maximal möglichen Abdeckung von "sensiblen" Bereichen hinsichtlich

- möglicher Schwere der Folgen,
- Auftretenswahrscheinlichkeit der Szenen und
- deren Kontrollierbarkeit.

Konzept für "sensible" Bereiche und Testfälle

- Zerlegung von ODD (Generierung von Szenarioinstanzen) basierend auf z.B.: "Kritikalitätsanalyse" kombiniert mit probabilistischen Analysen.
- Analyse relevanter Designelemente im Hinblick auf ihre Zuordnung zur Sicherheit.
- Komposition "sensibler" Bereiche durch Zusammenführung relevanter Design- und Szenariomerkmale.
- Generierung von Testfällen aus Design-Attribution und ODD-Analyse.

Validierung - Objektive: Überprüfung der Nutzenkonformität, Überprüfung von Grundannahmen auf denen die Entwicklung aufbaut, Überprüfung des integrierten Systems in einer stochastischen Umgebung.

Evaluierung des Restrisikos:

Abschätzung der Restrisiken (nach Verifikation) mit statistischen Methoden z. B. mittels Beinaheunfällen. Strategie: Zufällige ODD-Szenenauswahl bei gleichzeitiger Bestätigung der Vielfalt des Validationsspektrums.

Konzept zur Risikoabschätzung und Machbarkeit

- Das Restrisiko wird durch statistische Beschreibungen der Eintrittswahrscheinlichkeit von gefährlichem Verhalten oder Risiken einschließlich Signifikanzniveau bestimmt.
- Die Machbarkeit wird durch iterativ rückgekoppelte Schleifen in den Entwicklungsprozess erreicht, zum Beispiel wenn für die Sicherheit relevante jedoch bis dahin unbekannte Phänomene gefunden werden.
- Die Risikoschwellen werden in Übereinstimmung mit dem erforderlichen Sicherheitsniveau festgelegt.

V&V-Anwendung auf der Verhaltensebene basierend auf Framework

Der "V&V-Pfad" folgt den Perspektiven der Argumentation und damit den Schichten des Assurance Frameworks (Abbildung 141). Das beobachtete (monitored) Verhalten wird anhand des spezifizierten Verhaltens verifiziert und anhand des erforderlichen Verhaltens validiert. Voraussetzung ist die Validierung des überwachten Verhaltens gegen das reale Verhalten.

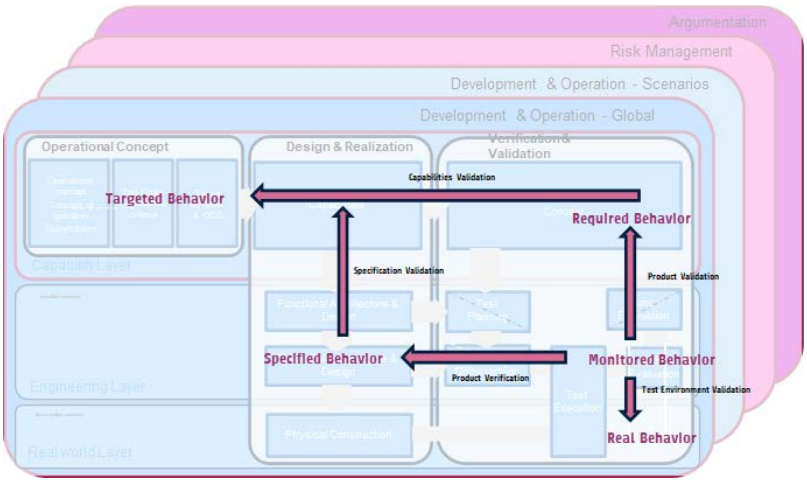


Abbildung 141: Pfad von V&V" dargestellt am Assurance Framework (© alle VVM)

Aggregationskonzept der Evidenzen

Die Aggregation der Evidenzen erfolgt im Wesentlichen im Rahmen der Argumentation, da die Argumentation die Zerlegung des Systems und seiner Risikomodellierung begründet. Die Aggregation im Rahmen der V&V Domäne aggregiert die Evidenzen soweit, dass diese in der Argumentation aufgenommen werden können. Hierbei werden Nachweise wie Testergebnisse, Methodenbewertung und Szenario-Exposition einbezogen.

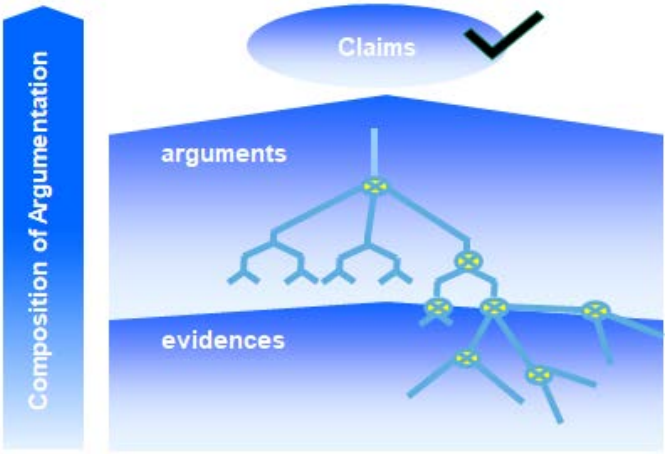


Abbildung 142: Zusammenfassung der Beweise entlang der Argumentation (© VVM)

3.1.1.9.3 Testplanung

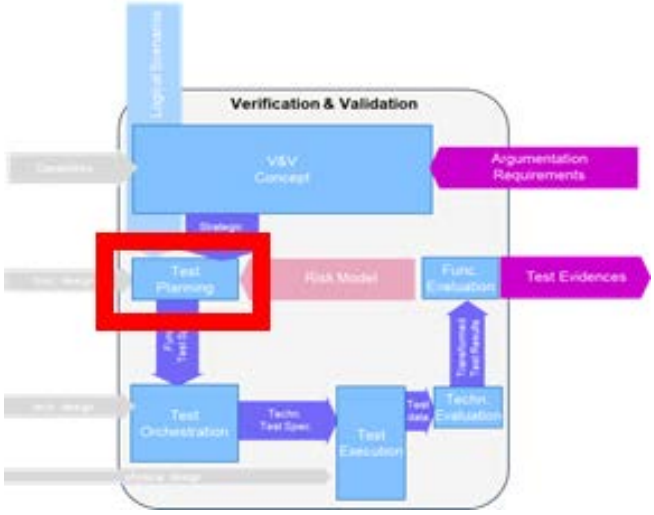


Abbildung 143: Testplanung im V&V-Konzept

Einführung

In der Testplanung wird die Menge aller funktionalen Testfälle definiert. Ein einzelner oder eine Gruppe gleichartiger funktionaler Testfälle wird durch eine funktionale Testspezifikation beschrieben, die alle für diesen Testfall oder diese Testfallgruppe relevanten funktionalen Testanforderungen bündelt. Die funktionalen Testspezifikationen stellen somit den funktionalen Testraum als zentrales Ergebnis der Testplanung dar. Im Wesentlichen geht es darum, die entsprechenden funktionalen Testobjekte und Szenarien auszuwählen und sie mit den gewünschten Testzielen einander zuzuordnen, d.h. mit Testfällen zu verbinden.

Strukturierung der Testplanung

Die Auswahl der funktionalen Testobjekte basiert auf dem funktionalen Entwurf der in Form einer funktionalen Architektur auf verschiedenen Abstraktionsebenen, auch funktionale Systemebenen genannt, beschrieben wird, und den damit verbundenen funktionalen Anforderungen einschließlich ihrer Qualitäten (siehe Abbildung 140). Die Testszenarien können aus der Gesamtmenge aller evaluierten Szenarien ausgewählt werden. Diese, im Kontext der VVM auch als "Logical Scenario

Instances" bezeichnet, repräsentieren die ODD vollständig und werden in ihrer Eintrittswahrscheinlichkeit bewertet.

Die Motivation für den Testfall wird in den Testzielen ausgedrückt. Zunächst wird hier grundsätzlich zwischen Verifikation und Validierung unterschieden. Während bei der Verifikation geprüft wird, ob das Produkt die Anforderungen erfüllt, geht es bei der Validierung um die Frage, inwieweit das Produkt seinen Verwendungszweck erfüllt. In beiden Fällen wird konkret beschrieben, was gemessen werden soll, um den für die Argumentation notwendigen Nachweis zu erbringen.

In der realen Welt sind die möglichen Kombinationen von Testobjekten, Umgebungen und Zielen endlos. Um sich auf eine in der Praxis umsetzbare Menge von Testfällen zu beschränken, wird eine Gewichtung nach den sicherheitssensitiven Bereichen vorgenommen. Dazu wird ein Modell benötigt, das die einzelnen Funktionen und Szenarien aus der Dekomposition von funktionalem Design und ODD hinsichtlich ihrer Bedeutung für die Sicherheit bewertet und quantitativ beschreibt.

Ein Sonderfall in diesem zunächst top-down strukturierten Ansatz sind die Bedenken. Dabei handelt es sich um Hinweise subjektiver (z. B. Bewertungen) oder objektiver (z. B. Messergebnisse) Natur, die hinsichtlich des Testumfangs besonders berücksichtigt werden müssen. Bedenken können in verschiedene Klassen eingeteilt werden. Funktionale Belange beziehen sich beispielsweise auf die funktionale Gestaltung, während Szenario-Belange sich auf Szenarien beziehen, die berücksichtigt werden müssen. Je nach Klassifizierung werden solche Bedenken an der entsprechenden Stelle aufgenommen, um ihre Sicherheitsrelevanz im Kontext des funktionalen Designs oder der logischen Szenarien-Instanzen zu gewichten.

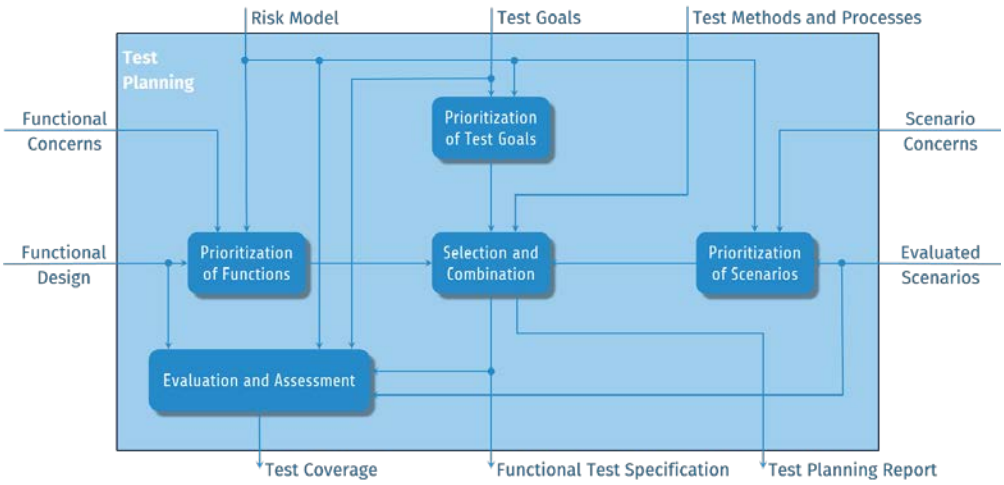


Abbildung 144: Strukturierung der Testplanung

3.1.1.9.4 Testorchestrierung

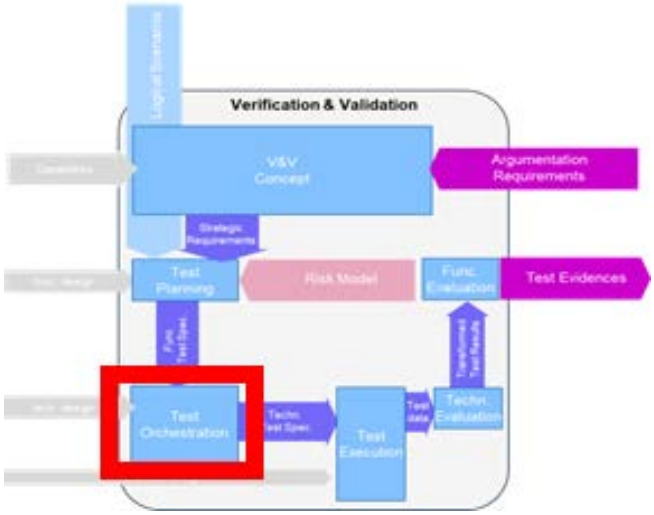


Abbildung 145:Testorchestrierung im V&V-Konzept

Für ein durchgängiges Testen von Fahrzeugfunktionalitäten stehen verschiedene Plattformen zur Verfügung. Diese reichen von der Simulation über X-in-the-Loop-Ansätze bis hin zu Fahrzeugen auf Testgeländen oder in der realen Welt. Eine Testorchestrierung ermöglicht durchgängige Tests und eine optimierte Nutzung verschiedener Testmethoden und -plattformen im Rahmen des V&V-Konzepts, wie in Abbildung 146 dargestellt.

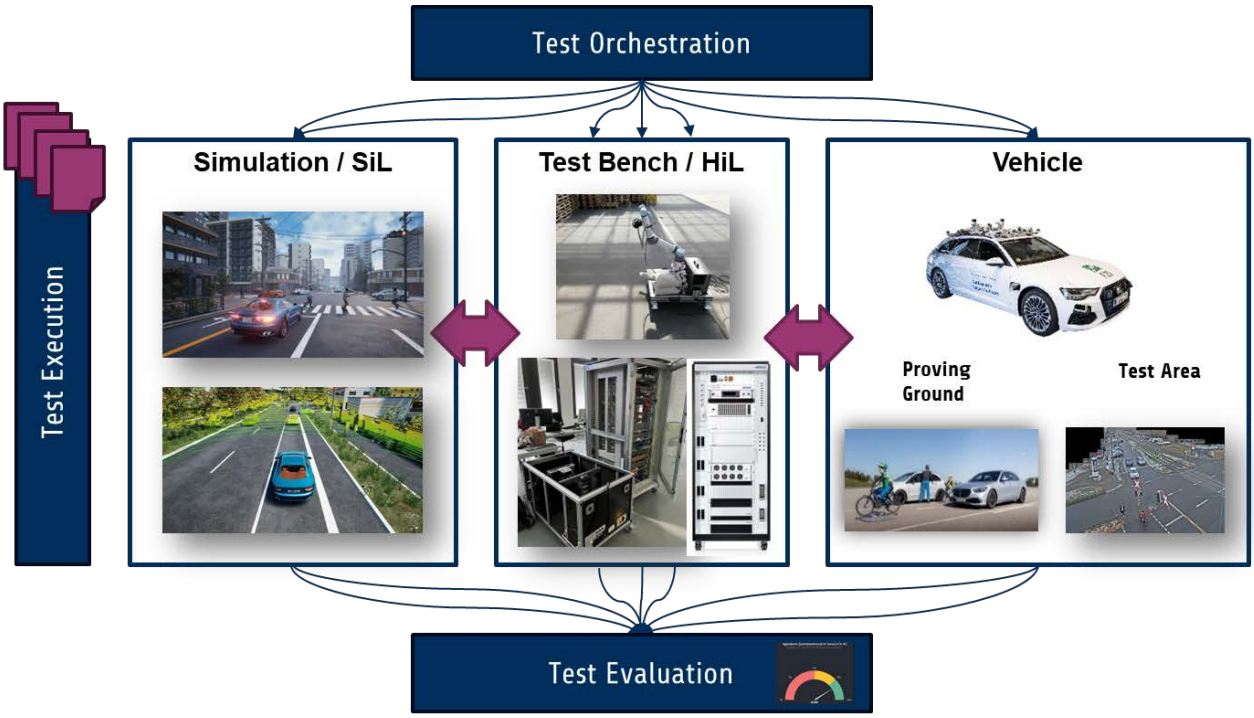


Abbildung 146: Testorchestrierung zur Ermöglichung „nahtlosen“ (seamless) Testens (© Fraunhofer LSB und FZI Forschungszentrum Informatik)

Die Testorchestrierung muss die Verbindung zwischen der Testplanung auf der einen Seite und der Testdurchführung auf der anderen Seite herstellen. Sie trägt damit dazu bei, dass die Sicherheitsargumentation bei der Umsetzung des V&V-Konzeptes vollständig durchgeführt werden

kann. Dabei muss sie stets folgende Punkte im Auge behalten: Effizienz, Durchführbarkeit, Validität und Abdeckung des Testraums.

Ziel ist es, technische Testspezifikationen zu generieren, die Testfälle auf den verschiedenen verfügbaren Testplattformen instanziieren.

Inputs in die Testorchestrierung

Die funktionale Testspezifikation liefert Informationen über das funktionale Testobjekt, die funktionalen Messgrößen und die relevanten Testszenarien.

Das technische Design liefert die technischen Systemanforderungen und die technische Architektur, die die jeweiligen Funktionen realisieren.

Das physikalische Design liefert die Information, wann und in welchen Konfigurationen integrierte Systeme für den Test bereit sind.

Schließlich wird das Wissen über die verfügbaren Testplattformen bereitgestellt: Verfügbarkeit, Gültigkeit, Betriebsgrenzen und Effizienz.

Output: Die technische Testspezifikation

Die technischen Testspezifikationen sind die Dokumente, die zwischen der Testorchestrierung und der Testdurchführung ausgetauscht werden. Jede technische Testspezifikation liefert die Information, welches physische Testobjekt und welche konkreten Szenarien auf welcher Testplattform instanziiert werden sollen, um welche physikalischen Messgrößen zu messen (siehe Abbildung 147).

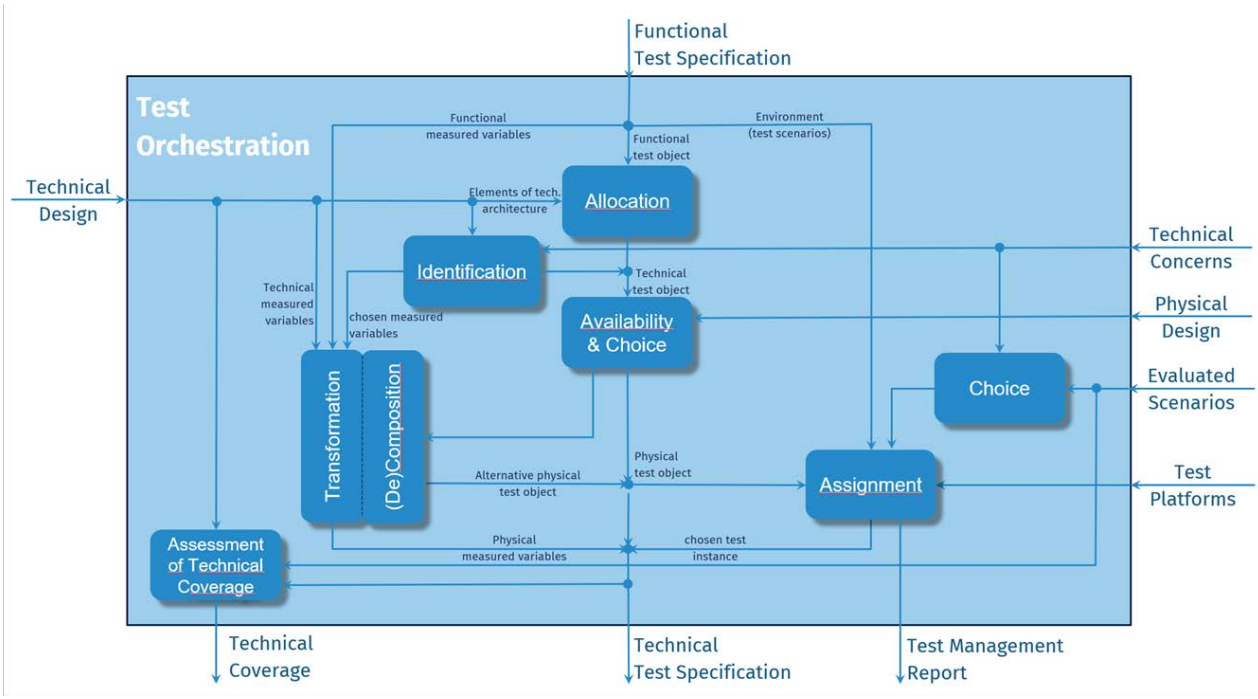


Abbildung 147: Prozess der Testorchestrierung

Der Kernprozess der Testorchestrierung

In Abbildung 147 ist der Prozess der Testorchestrierung dargestellt. Dieser ist sowohl für die Verifikation als auch für die Validierung anwendbar. Der Kernprozess umfasst die folgenden Schritte:

Allokation - Identifikation des technischen Testobjekts auf Basis des spezifizierten funktionalen Testobjekts durch Verfolgung der Zuordnung der funktionalen Architekturelemente zu den technischen Architekturelementen aus dem Entwurfsprozess.

Transformation - Daraus werden anhand der funktionalen Key Performance Indicators die zu untersuchenden technischen Parameter extrahiert, d.h. die funktionalen Messgrößen werden in die konkreten physikalischen Messgrößen übersetzt.

Verfügbarkeit & Auswahl - Anhand des technischen Prüfobjekts, das in Form einer Beschreibung einer Art theoretischen Modells vorliegt, wird die Verfügbarkeit und Eignung des entsprechend der Konfiguration geeigneten und realisierten physikalischen Prüfobjekts überprüft.

Zuordnung - Unter Berücksichtigung von Kriterien wie Machbarkeit, Aufwand, Kosten, Verfügbarkeit und Validität wird die Testplattform ausgewählt und das physikalische Testobjekt und die Testszenarien werden auf der Testplattform instanziiert und damit die Testinstanz aufgebaut.

3.1.1.9.5 Test execution and evaluation

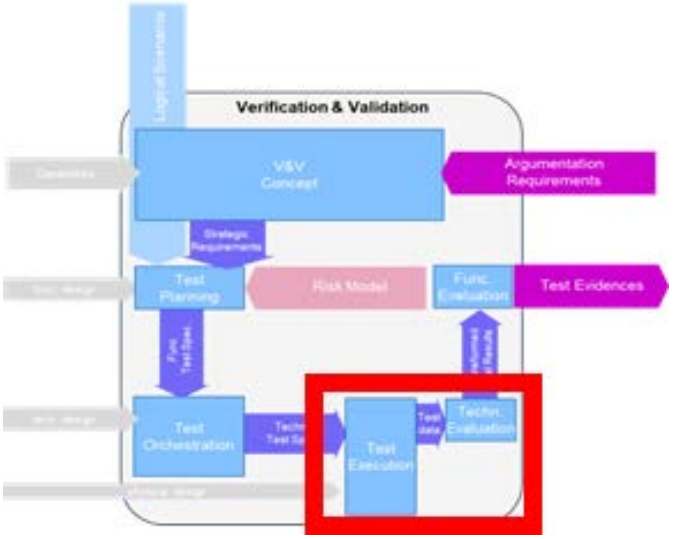


Abbildung 148: Testdurchführung im V&V-Konzept

Seamless Testing

Die Testdurchführung erfolgt nach den im Rahmen der Testorchestrierung festgelegten technischen Testspezifikationen. Die einzelnen Durchführungen erfolgen parallel auf verschiedenen spezifizierten Testplattformen nach dem Prinzip des durchgängigen Testens. Dabei sind die folgenden Aspekte zu berücksichtigen:

Komplementarität: Alle Tests müssen sich in ihren Ergebnissen gegenseitig ergänzen. Insgesamt müssen alle Testergebnisse in ihrer Gesamtheit den schlüssigen Nachweis der Sicherheit und Konformität des ADS gewährleisten. Es darf keine Lücke geben. Überschneidungen zwischen den Tests müssen kontrolliert werden. Ein Beispiel ist die mechanische Vibration einer

Kameraperzeption. Dies kann im Rahmen eines spezifischen Hardware-in-the-Loop-Tests abgedeckt werden, wie in Abbildung 1 dargestellt. Die Tests in der realen Welt und die Tests, die innerhalb der spezifischen HiL-Testplattform durchgeführt werden, müssen sich gegenseitig ergänzen, um eine fundierte Argumentation zu gewährleisten.

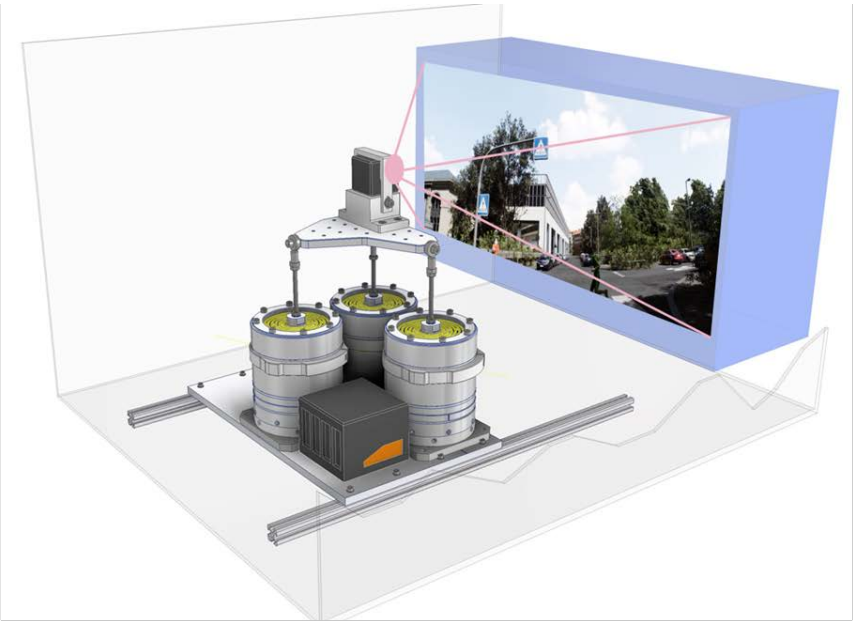


Abbildung 149: HiL-Testplattform für den Einfluss mechanischer Vibrationen auf die Perzeption. (© Fraunhofer LSB und FZI Forschungszentrum Informatik)

Effizienz: Die optimale Testverteilung wird gewählt, um Zeit- und Kosteneffizienz zu erreichen. Einerseits erfordern Tests in der realen Welt einen hohen Aufwand und müssen sehr gut geplant werden, sind dafür realistisch und effektiv, andererseits sind Simulationen effizienter, aber weniger realistisch, wie in Abbildung 2 dargestellt.

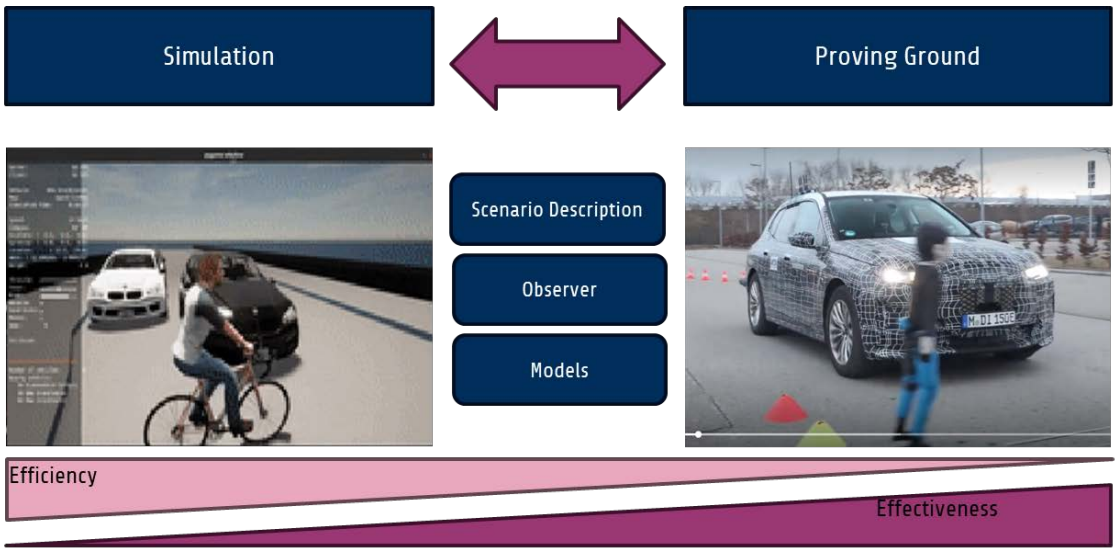


Abbildung 150: Symbiose auf Simulations- und Realtest (© BMW AG)

Wiederverwendbarkeit von Testressourcen: Die Verwendung z.B. eines Simulationsmodells muss gegebenenfalls in verschiedenen Testinstanzen möglich sein.

Konsistenz: Alle Testergebnisse müssen konsistent sein. Es darf keine widersprüchlichen Testergebnisse geben.

Flexibilität: Verschiedene Testinstanzen können sich gegenseitig ersetzen.

Testauswertung

In Anlehnung an das zweistufige Verfahren zur funktionalen und technischen Planung von Tests wird auch die Auswertung in einen funktionalen und einen technischen Schritt unterteilt.

Die technische Auswertung entspricht der Testorchestrierung. Auf dieser Ebene werden die bei der Durchführung der Tests erzeugten Testdaten technisch ausgewertet. Da die technischen Schnittstellen und Signale nicht notwendigerweise den Funktionalen entsprechen, ist analog zum Schritt von der funktionalen zur technischen Spezifikation auch eine Rücktransformation der technischen Messwerte in Funktionale notwendig. Somit wird der Ansatz der Architektur-, Design- und Testplanung zur Trennung von funktionalen und technischen Aspekten mit all seinen Vorteilen auch bei der Auswertung konsequent verfolgt.

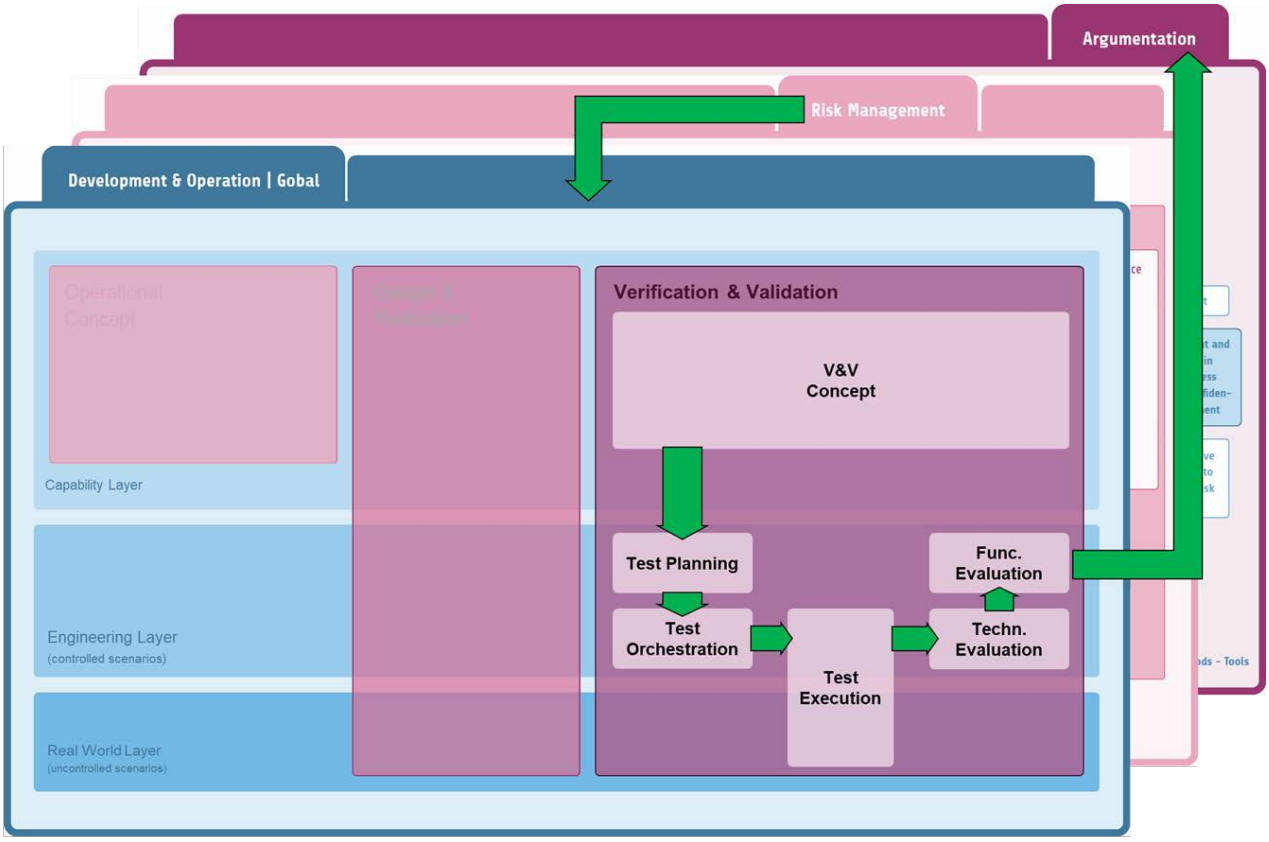


Abbildung 151: Fokus der Test Evaluation

Schließlich wird durch Aggregation aller Bewertungsergebnisse eine ganzheitliche Aussage zur Sicherheit, das heißt vollständig in Bezug auf das Produkt, sein Betriebsumfeld und die verfolgten Sicherheitsziele, generiert. Für diese Verdichtung der Bewertung wird dasselbe Modell verwendet, nach dem zuvor die Sicherheitsanforderungen in Komponenten, Szenarien und Teilziele zerlegt wurden. Dieses Modell befindet sich im Block "Risikomanagement" des Assurance Framework.

3.1.2 Überblick über die VVM-Gesamtmethode

3.1.2.1 TP1 Rahmenbedingungen und Impulsgeber

Das Teilprojekt 1 stellt als übergreifendes Teilprojekt Rahmenbedingungen bereit und entwickelt eine gesamtheitliche Projektperspektive, die als Impulsgeber und Ordnungsfunktion für das Gesamtprojekt im Bereich der Methodenentwicklung dient. Insbesondere werden Ergebnisse aus früheren Förderprojekten auf Relevanz und Verfügbarkeit geprüft und als Stand der Technik herangezogen. Im Weiteren bildet TP1 in Zusammenarbeit mit dem TPX die zentrale Kommunikationsschnittstelle des Projektes nach außen. TP1 ist sowohl nach innen wie nach außen der organisatorische Anker des Gesamt-Projekts.

Neben dem technisch-inhaltlichen Rahmen stellt TP1 auch den Rahmen für die Zusammenarbeit im Konsortium her, in einer Brückenfunktion fördert es das Zusammenwirken der Teilprojekte im Hinblick auf das Erreichen der strategischen wie operativen Projektziele.

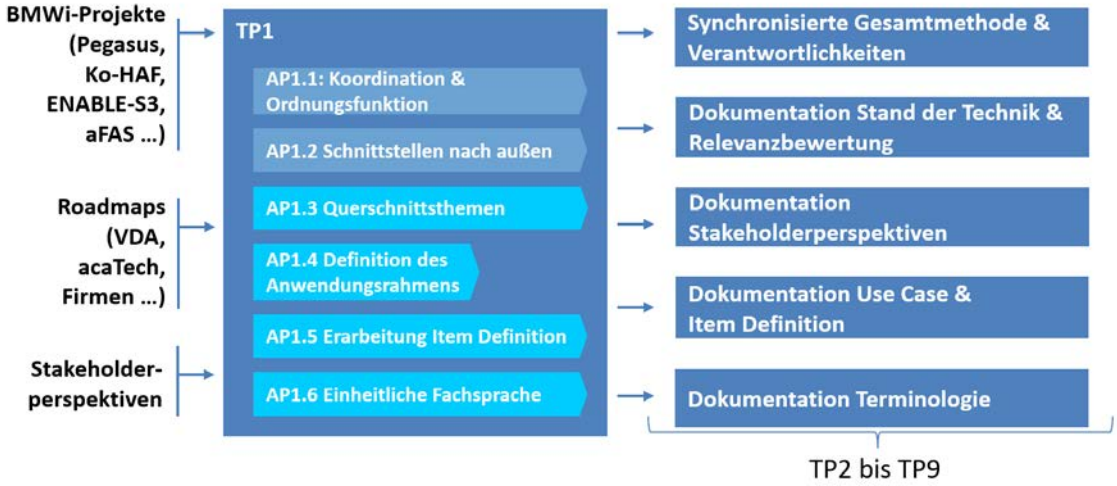


Abbildung 152: Darstellung der Grundstruktur Teilprojekt TP1

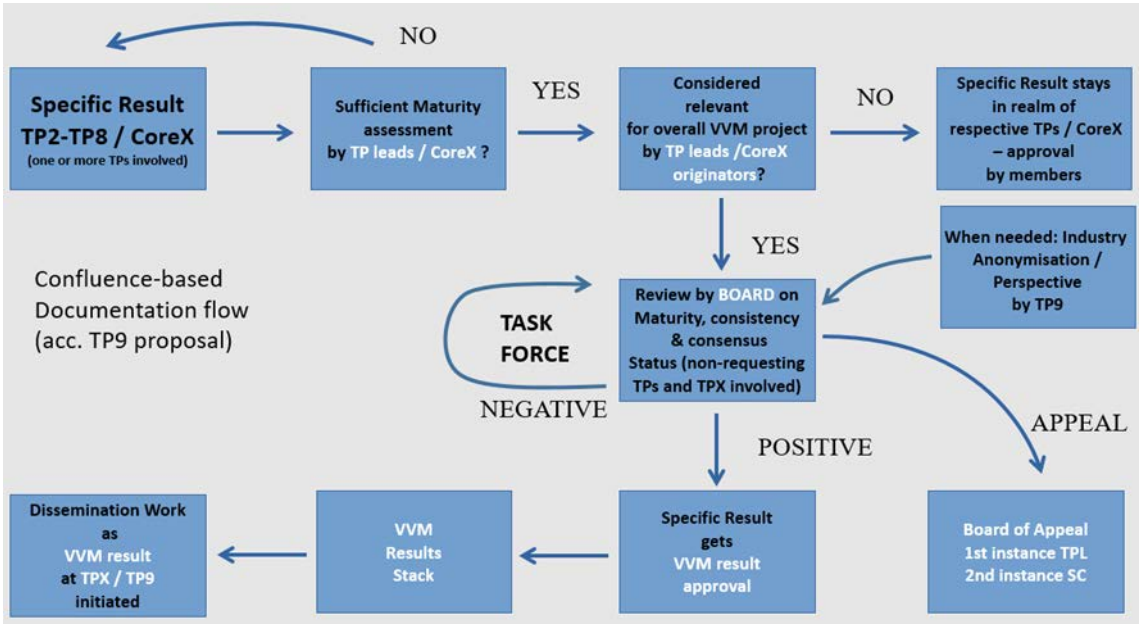


Abbildung 153: Struktur des BOARD-Prozesses zur projektinternen Ergebnisverbreitung und Genehmigung von offiziellen VVM-Ergebnissen

Results-BOARD: Übersicht der Projektergebnisse zum Review

Erstellt von Dr Christian Bühler, zuletzt geändert von Nayel Salem gestern um 10:49 AM

Diese Seite bietet einen Überblick über die im Projekt erarbeiteten Ergebnisse, die für den Review im Results-Board vorgelegt werden sollen. Darüber hinaus dient sie auch als Übersicht für Ergebnisse bei denen der Review Prozess bereits abgeschlossen wurde. Es wird dabei zwischen Ergebnissen unterschieden, die den Review erfolgreich abgeschlossen haben und als damit als Teil der VVM-Results-Stack angesehen werden und Ergebnissen, die im Rahmen des Board of Appeal einer weiteren Betrachtung und unterzogen werden. (siehe hierzu auch Prozess zur Ergebnisverbreitung)

Prozess

Arbeitshinweise zur Verwendung der Seite:

- Das Board Meeting findet alle vier Wochen Mittwochs von 15:00 - 16:00 statt.

⚠ **Einwahldaten für das Board-Meeting**
https://global.gotomeeting.com/join/909675829
Deutschland: +49 891 2140 2090
Direktwahl: tel:+4989121402090,,909675829#
Zugangscode: 909-675-829

- Ein Ergebnis, dass im Board Meeting vorgestellt werden soll, wird vom ergebniserstellenden Partner in die unten stehende Tabelle selbstständig unter "***Name: VVM-Result***" eingetragen
- Weitere erforderliche Teilnehmer, die über den Kreis des Results-Board hinaus gehen, können sich unter "***Zusätzliche Teilnehmer***" eintragen oder auf Wunsch vom ergebniserstellenden Partner eingetragen werden
- Die möglichen Status für die Ergebnisse sind: **Bereit für Review**, **VVM-Result** und **Board of Appeal** (basierend auf dem Review des Results-BOARD)
- Nach Annahme im Results-Board bitte den "***Link zur Ergebnisseite***" mit einfügen
- ***Ergebnisbacklog*** dient zur initialen Sammlung der Projektergebnisse

Übersicht der Projektergebnisse

Termin: Board Meeting	Name: VVM-Result	Ergebnis-verantwortlicher / Ergebnis-verantwortliches TP	Zusätzliche Teilnehmer	Status: VVM Result	Link zur Ergebnisseite (Results-Stack)
20.01.2021	Funktionale Architektur	Tamara Hofmann		VVM-RESULT	D02: Entwurf Systemarchitektur
verschoben auf 07.04.2021	VVM Safety Argumentation Structure	Jan Reich		IN PREPARATION	PDF
28.04.2021		abgesagt		IN PREPARATION	
16.06.2021	Wordversion von Deliverable D02	Tamara Hofmann		IN PREPARATION	
30.06.2021	PSM Formalismus	Hans Nikolaus Beck		IN PREPARATION	Präsentation

Abbildung 154: Confluence-Dokumentation der Vorträge im Rahmen des BOARD-Prozesses.

AP1.1 übernimmt die Projektkoordination sowie die Spiegelung des Stands der Technik zu Beginn des Projekts und evaluiert und synchronisiert die Gesamtmethode zu mehreren Zeitpunkten im Projektverlauf. Unter anderem wurden hier die Aktivitäten zur Unterstützung der Arbeiten an der Gesamt-Methode via projekt-übergreifenden Arbeitsgruppen gesteuert.

Das AP1.2 behandelt die Schnittstelle zur Kommunikation mit den Fördergebern, Ministerien, VDA-LI und anderen Stakeholdern sowie öffentliche Workshops zur Sicherstellung einer breiten Akzeptanz des Stands der Technik, der durch VVMethoden erarbeitet wird. Aktivitäten der externen Kommunikation auch im Rahmen des Abschlussevents spielen hier eine große Rolle.

Das AP1.3 ist für die Bearbeitung von Querschnittsthemen verantwortlich. Dazu mussten die Themen identifiziert, abgegrenzt und über den Projektverlauf koordiniert werden. In diesem Zusammenhang wurden die gesamtprojekt-übergreifenden Themen und Schnittstellen zwischen den Teilprojekten definiert und strukturiert.

Im AP1.4 wurden die funktionalen Use Cases sowohl bezogen auf die Form als auch den Inhalt erarbeitet. Dies geschieht in enger Zusammenarbeit mit dem TP2. Der Use Case 2.3 diente als das große zusammenhängende Strukturelement des Gesamtprojekts, sowohl in der Arbeit nach innen als auch nach außen.

Das AP1.5 setzt auf der Definition des Funktionsumfangs auf und formalisiert diesen in eine Item Definition in Anlehnung an die Norm ISO 26262. Aus der Beschreibung und zusammen mit Projektergebnissen vorangegangener Projekte (z.B. aFAS und PEGASUS) können Gütekriterien für die Bewertung von Sicherheit im Use Case Urbane Kreuzung identifiziert werden.

Um ein einheitliches Verständnis der Konzepte und Methoden zu schaffen, wird im AP1.6 eine einheitliche Fachsprache erarbeitet.

Die Aktivitäten zum Glossar zeigten sich von großer Wichtigkeit für das Gesamtprojekt im Sinne der Schaffung der inhaltlichen Fachsprache, um die Projektergebnisse intern und extern zu kommunizieren, wie etwa im Rahmen der Abschluss-Veranstaltung in Stuttgart (siehe Abbildung

2). Die an den übergeordneten TP1-Gesamt-Kreis berichtende Arbeitsgruppe hat das Glossar in Zusammenarbeit mit SetLevel und Vivaldi speziell mit Begriffen der Gesamt-Argumentation und -Methode erweitert. Auch der Austausch mit Gaia-X Projekten wurde fortgeführt. All dies geschah abgestimmt mit dem Teilprojekt TPX, mit dem diesbezüglich eine enge Kooperation besteht.

Der von TP1 vorangetriebene und koordinierte BOARD-Prozess zur Erreichung VVM-weiter Konsens-Positionen und zur Ergebnis-Visibilität eine sehr große Rolle, besonders wenn sich in Teilprojekten zwischenzeitlich unterschiedliche Sichtweisen aufgetan hatten. Der BOARD-Prozess wurde im Sinne einer Setzung der Rahmenbedingungen durch TP1 mit Unterstützung von TP9 (siehe Abbildung 1a) geschaffen. Bei diesem Prozess geht es darum für relevante Projektzwischen-Ergebnisse eine projektübergreifende Öffentlichkeit zu schaffen, um eine ebenfalls projektübergreifende Zustimmung zu diesen Ergebnissen via eines konsensualen Prozesses zu erreichen. Dies ist von besonderer Bedeutung auf Grund der neuen Arbeitsgruppen, die sich aus Mitgliedern verschiedener Teilprojekte zusammensetzen, welche mit Aufträgen ausgestattet wurden. Zudem hat das „BOARD-Meeting“ die Funktion als eine Art Review-Gremium für Projekt-Deliverables zu dienen: Wenn dieses Gremium ein Projektergebnis bestätigt wird es in den so genannten „VVM Results Stack“ aufgenommen. Ergebnisse, die sich darin befinden können als Basis für die Dissemination durch die Projektpartner intern, sowie durch TP9 und TPX dienen. Zur Dokumentation wurde ein eigener Bereich auf dem Kollaborations-Werkzeug „Confluence“ geschaffen, auf dem sowohl die Vortragspräsentationen als auch die Aufzeichnungen der gehaltenen Vorträge dokumentiert wurden.

Die Frequenz der BOARD-Meetings nahm im Projektverlauf besonders hin zum Finalevent in Stuttgart deutlich zu, da nun mehr und mehr im Projekt erarbeitete Ergebnisse vorgestellt und abgestimmt werden konnten und mussten.

Die Abschlusspräsentation wurde organisatorisch im TP1 geplant, wobei am ersten Tag die VVM-Projektergebnisse im Vordergrund standen, während am zweiten Tag die internationalen Kooperationen den Fokus bilden. Hierfür wurde als exemplarisches Beispiel u.a. eine Publikation „Cross Domain Safety Assurance Framework for Automated Transport Systems” aus dem Vereinigten Königreich analysiert, welches nicht nur den Automobilbereich, sondern alle Transportsektoren adressierte. Wenn es doch auch Abweichungen im Detail gab, so wurde eine große prinzipielle Vereinbarkeit sowohl was Methode als auch Fachsprache betrifft festgestellt. Das gilt besonders für die Strukturierung des Operational Domain respektive Design Domain als auch generell für die szenariobasierte Methode und die Anwendung von Szenarien-Datenbanken.

Die in Zusammenarbeit mit TPX geführten Gespräche, u.a. mit den französischen und britischen Aktivitäten zu Szenario-Datenbanken wie ADScene und SafetyPool oder mit dem Forschungsbereich des Verbands deutscher Verkehrsunternehmen, im Hinblick auf potenzielle Anwendungen von AD-Technologien und deren Sicht auf spezifische Szenarien im ÖPNV oder Datenbank-Ansätzen wurden im TP1 unterstützt. Arbeitsschwerpunkt besteht in der Konsolidierung der Projektergebnisse und der intensiven Vorbereitungsaktivitäten für das Abschluss-Event (siehe Abbildung 155).

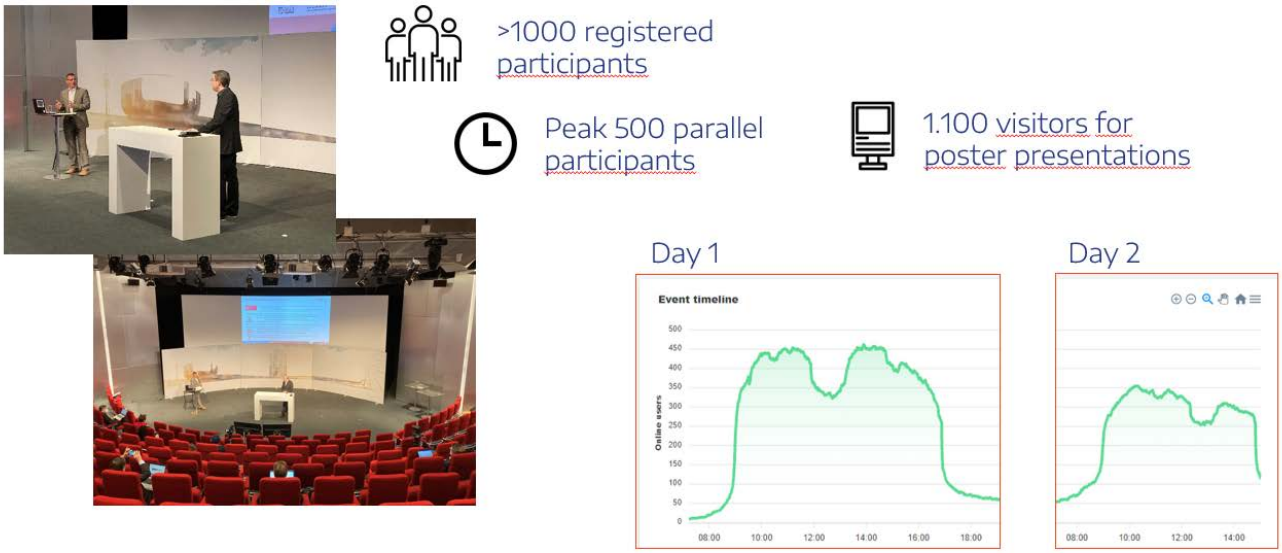


Abbildung 155: Halbzeit-Event im BMW Technology Centre in München

Abbildung 156: Abschluss-Event in der Carl-Benz-Arena in Stuttgart

Im Hinblick auf die Kommunikation nach außen waren die Halbzeitveranstaltung in München im März 2022 im BMW-Technologiezentrum sowie die Abschlussveranstaltung in Stuttgart im November 2023 in der Carl Benz Arena, aufbauend auf die offenen internationalen PEGASUS Expert Workshops, sicher die Höhepunkte des Projekts. Zur Zwischenpräsentation in der schwierigen Phase der Ausläufer der Covid-Pandemie konnte in einem virtuellen Format der Stand des Projekts in hoher Reichweite international die Ergebnisse sowie die globalen Kollaborationen vorgestellt werden. Von externen Beobachtern wurde eine inhaltlich äußerst interessante und professionelle Veranstaltung konstatiert. Auch bezüglich der Anzahl der Teilnehmenden an beiden Tagen mit mehr als 1000 Registrierungen war das Event eine äußerst erfolgreiche Veranstaltung, es konnte durchgehend über beide Tage eine sehr hohe Zahl sichergestellt werden. Das Konzept der hybriden Veranstaltung hat sich für das Halbzeit-Event zu diesem Zeitpunkt sehr bewährt, es gab dadurch keine Verwerfungen durch die zu diesem Zeitpunkt grassierende Welle der Corona-Pandemie.

Zur Abschlussveranstaltung in Stuttgart konnte wieder auf das Konzept eines physischen Events zurückgegriffen werden. An beiden Tagen in Stuttgart waren ca. 400 Personen in der Carl-Benz-Arena vor Ort und konnten persönlich teilnehmen und auch die Möglichkeiten zum direkten

persönlichen Kontakt nutzen. Der erste Tag diente im Wesentlichen der Kommunikation der VVM-Ergebnisse, und Tag 2 fokussierte sich in Zusammenarbeit mit TPX auf die Vorstellung internationaler Partnerinitiativen u.a. aus den USA, Japan, UK, Frankreich und der EU. Durch den Erfolg der virtuellen Halbzeitpräsentation zeigte sich wie wichtig eine globale internationale Visibilität durch eine Online-Präsenz ist, wurde auch beim Abschlussevent eine virtuelle Komponente vorgesehen. Obwohl der Schwerpunkt der Stuttgarter Veranstaltung auf dem physischen Event war, war auch diese virtuelle Kommunikation ein großer Erfolg. An beiden Tagen waren zusätzlich mehrere hundert Teilnehmer aus dem internationalen Umfeld so bei PEGASUS VVM präsent.

Die Vorträge, Präsentationen und Poster des Abschlussevents sind unter https://www.vvm-projekt.de/en/final-event verfügbar. Die Vorträge und Podiumsdiskussionen sind dort sowohl als Aufzeichnung als auch mit den gezeigten Foliensätzen archiviert.

Die erarbeiteten „Functional Use Cases, insbesondere der Functional Use Case 2.3. sind essenziell für die VVM-Aktivitäten über die Methodenarbeit bis zur simulativen und experimentellen Umsetzung hinaus. Auf diesen Use Cases aufbauen wurden die notwendigen Adaptionen für das ursprüngliche 6-Layer-Modell erarbeitet, ebenso dienten diese als Ausgangspunkt für die Schaffung der von VVM in Teilprojekt 2 vorgeschlagenen A.U.T.O-Ontologie. Bezüglich der experimentellen Umsetzung in den höheren Teilprojekten via Simulation und Prüfgelände bzw. Realwelttest dienten die FUC ebenfalls als Leitstern. Auch bei der Abschluss-Veranstaltung und den Planungen hierfür dienten die FUC 2.3 und 2.4 wiederum als Basis. Für die VVM-Gesamtmethode und den so genannten Szenarien-Strang hat das das „Functional-Use-Case“-Dokument eine bedeutende Funktion, ebenso wie für die Strukturierung des zentralen Begriffes der „Operational Domain“ bzw, des „Operational Design Domain“ (siehe Abbildung 157), welcher bei der Fahrzeug-Automatisierungstechnik eine Schlüssel-Rolle spielt, dies zeigt sich u.a. auch in der Zusammenarbeit mit den globalen Partner-Initiativen.

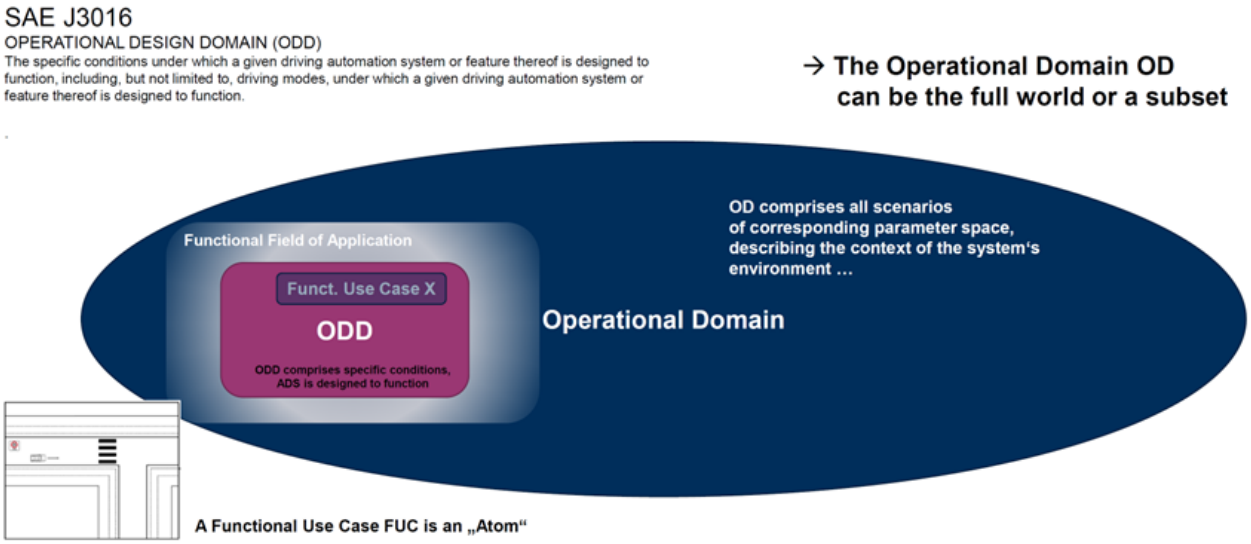


Abbildung 157: Zusammenspiel „Functional Use Case“ und Operational Domain/Operational Design Domain

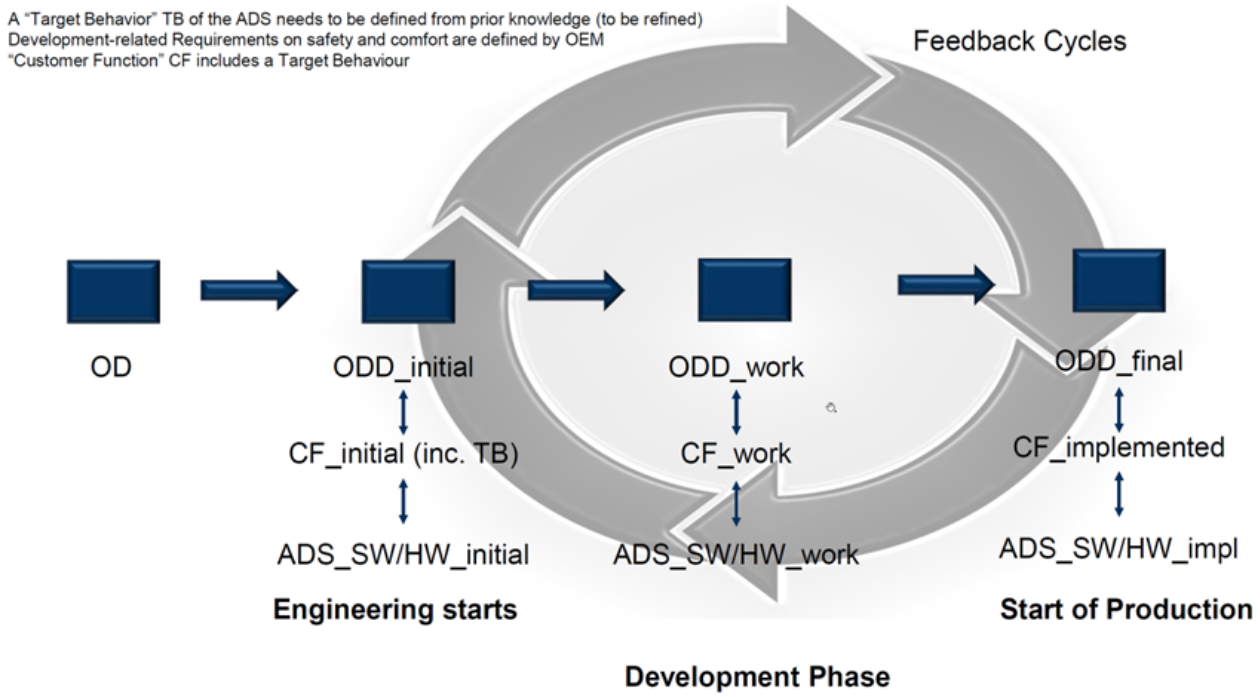


Abbildung 158: Zusammenspiele unterschiedlicher Reifegrade von Kundenfunktion, ODD und technischer Implementierung

In TP1 wurde weiterhin verstärkt am verbesserten Zusammenspiel zwischen „Item Definition", der begrifflich neu definierten Kundenfunktion und der daraus resultierenden Projekt-sowie ADS-Architektur gearbeitet. Auch hier zeigt sich in den projekt-internen und -externen Diskussion die Wichtigkeit von Konzepten wie etwa der „Kundenfunktion" für das zu untersuchende „System-under-Test".

Abschließend wurde in TP1 der VVM-Glossar-Prozesse aufgesetzt und gelebt. Dies führte zu sehr positiven Ergebnissen im Sinne eines konsensualen Vorgehens innerhalb des Projekts und mit Partner-Initiativen wie SetLevel, Vivaldi/Vivd und Gaia-X. Jeder VVM-Teilnehmer hatte die Möglichkeit am gemeinsamen Begriffsregister mitzuwirken. Die Mitwirkung konnte über den AP-Leiter, Kommentare im Arbeitsdokument oder gemeinsame Konsultationen erfolgen. Die breite Einbindung war notwendig, um Begriffe in einem konsensualen Prozess festzulegen. Im Fall von Meinungsverschiedenheiten wurde ein Konfliktauflösungs-Prozess etabliert. Mehr als 100 Begriffe konnten in das abgestimmte Glossar überführt werden. Die Übersetzung für das Glossar wurde in Zusammenarbeit mit TPX in Auftrag gegeben, um eine zweisprachige Verfügbarkeit auf Englisch und Deutsch sicherzustellen. Zusätzlich zu den Konsultations-Meetings wurden diese Sitzungen im Vorfeld vor- und nachbereitet, um den Projekt-Konsens zu erreichen, sowie an der technischen Umsetzung des lebenden Dokuments in Form eines interaktiven Glossar-Dokuments. Zudem konnte durch diese die Umstellung des Glossars auf ein mit einer Suchfunktion und Hypertext-Link-Funktionalität ausgestattetes Format, die Nutzbarkeit für den Anwender deutlich verbessert werden (Siehe https://zenodo.org/records/10533077 und Abbildung 4)

Status	Änderung	Begriff	Term engl.	Abbr	Intention	Was wird mit dem Begriff gemacht (Intention detailliert)	Erläuterung	Bezogene Gegenstände	Bezogenene Subjekte	Subjekt (Adressat)
					Beschreiben		Informationsquellen zur Erstellung eines Weltmodells.	Architektur		
Akzeptiert	08.12.2020	Zu testende Perzeption bzw. Perception under Test	Perception Under Test	PUT	Benennen	Unterscheidung verschiedener Datenquellen	Zu testende Software bzw. Algorithmen, die "Sensorik under Test"-Rohdaten zu Umfeldmodell-Daten verarbeitet.	Algorithmus, Neuronales Netzwerk		Personen, die Perzeptionsda arbeiten
Akzeptiert	08.12.2020	Perception under Test Daten	Perception Under Test Data	PUT Data	Benennen	Unterscheidung verschiedener Datenarten	Daten des Typs "Environment Model Data" aus der Quelle „Sensor(s) under Test". Ergänzung: In VVM können diese Daten auf zwei verschiedene Weisen aus den SRD generiert werden: Entweder durch bereitgestellte Perzeptionsalgorithmen der Forschungspartner oder durch vom Hersteller integriertes Objekttracking o.ä. in den Sensor(s) under Test.	Verkehrsumfeld		Personen, die Perzeptionsda arbeiten
Akzeptiert	04.02.2020	Phänomen	Phenomenon		Beschreiben	Personen arbeiten nicht wie Videokameras, sie nehmen ein Geschehnis auf der Basis ihrer Erfahrungen und Interessen wahr. Das Geschehnis wird erlebt, und das Erlebte wird bezogen auf andere Sachverhalte oder Erfahrungen der Person. Diesen Sachverhalt und damit die Subjektivität im Verkehrsgeschehen zu beschreiben ist Sinn des Begriffs Phänomen. Daraus folgt, dass bei Beschreibung eines Phänomens auch die Benennung der wahrnehmenden Subjekte erfolgen muss.	Beschreiben von Geschehnissen in der Verkehrswelt, die einem subjektiven Erleben entsprechen. Die Beschreibung ist keine objektive Erfassung aller Aspekte des Geschehnisses, sondern ist wahrgenommen bzw. erlebt durch eine oder mehrere Personen auf dem Hintergrund eines Interesses oder des Zustandes dieser Person(en). Grundlage ist das unmittelbare Erleben des Subjektes Beispiel: Als Fußgänger nehme ich Autos anders wahr als Autofahrer.	Geschehen im Verkehr, Gleichzeitigkeit (Koinzidenz) im Verkehr, Handlungsweisen von Mitmenschen im Verkehr; nicht erwartete Ereignisse, Dinge	Verkehrsteilnehmer aller Verkehrsmittel und Altersgruppen	Unfallforscher Verkehrsplane Anforderungs
Akzeptiert	22.02.2021	Phase	Phase		Beschreiben		Eine Phase ist eine Unteraktivität in einem Prozess und setzt sich aus mindestens einem Task zusammen.			TRACY
Akzeptiert	07.06.2022	Physikalische Domäne	Physical Domain		Beschreiben		Betrachtung der konkreten Umsetzung (Konfiguration), die die technischen Anforderungen erfüllt und die technischen Schnittstellen bedient.			
Akzeptiert	30.11.2022	Physikalisches Design	Physical Design		Beschreiben		Physikalische Realisierung des technischen Designs.			

Abbildung 159: Strukturierung des Glossars für die technische Fachsprache, in zusätzlicher Abstimmung mit Partnerinitiativen

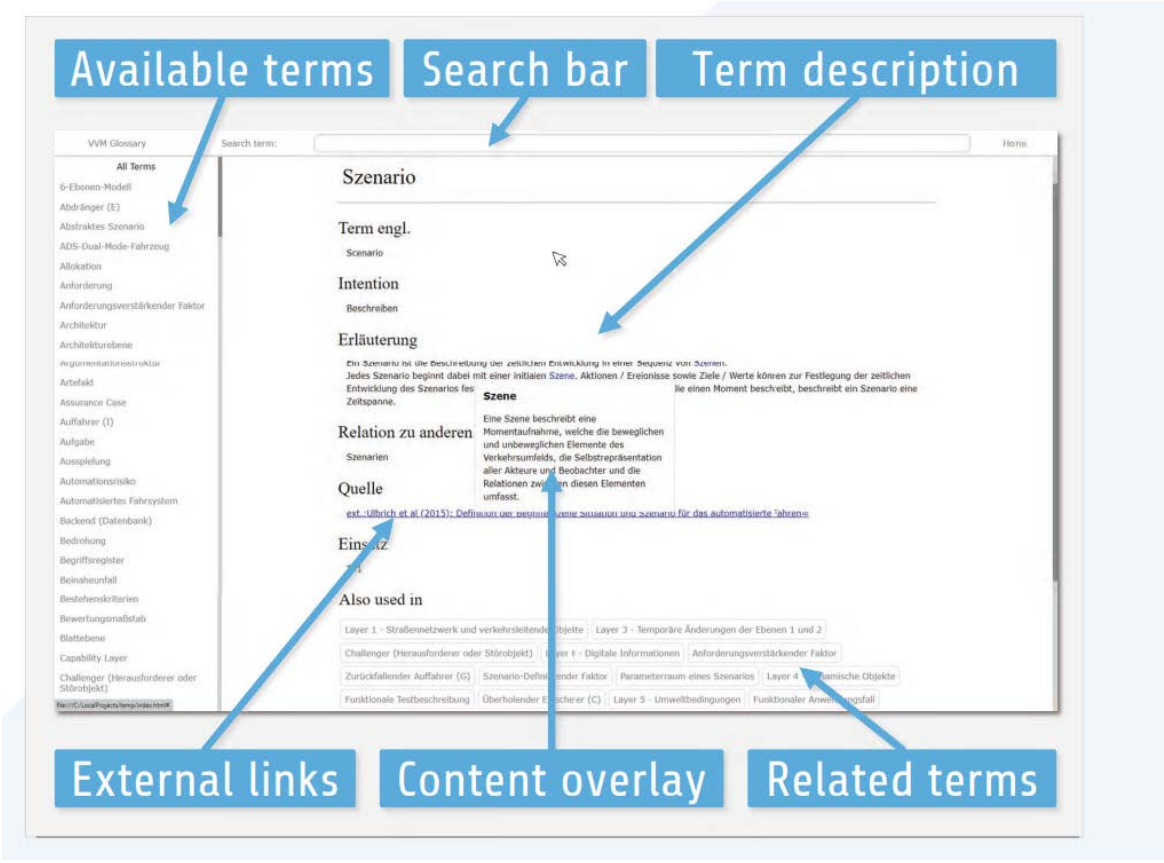


Abbildung 160: Aufbau der grafischen Benutzeroberfläche des PEGASUS-VVM-Glossars in Form eines „lebenden“ Dokuments

Die detaillierten inhaltlichen Aktivitäten im Sinne des VVM-Fraemwork, die aus dem TP1 heraus koordiniert wurden, sind in den übergreifenden Kapiteln dieses Abschlussberichts zur VVM-Gesamtmethode dokumentiert.

3.1.2.2 TP2 Kritikalitätsanalyse

3.1.2.2.1 Zusammenfassung der TP2-Arbeiten

Die TP2 Arbeiten sind in großen Details in den folgenden, frei zugänglichen Dokumenten beschrieben:

- Deliverable D01: Criticality Analysis for the Verification and Validation of Automated Vehicles
- Deliverable D08: Advances on the Criticality Analysis for Automated Driving Systems
- Deliverable D09: Requirements on Simulation Systems and Models Posed by a Criticality Analysis for Automated Driving Systems

Im Folgenden fassen wir die erzielten Ergebnisse geordnet nach den Arbeitspaketen AP2.1, AP2.2, AP2.3, und AP2.4 kurz zusammen.

3.1.2.2.2 AP2.1 - Charaktersierung des Szenarienraums und Ontologie für Szenarienannotation

3.1.2.2.2.1 E2.1a - Draft Version Ontologie

Direkt zu Projektstart wurden die Arbeiten an der in VVMethoden entwickelten Ontologie Automotive Urban Traffic Ontology (A.U.T.O.), welche das 6-Ebenen-Modell aus PEGASUS erweitern und für den urbanen Verkehr anpassen soll, unter der Koordination von OFFIS gestartet. Nach Einfinden eines Core-Teams und anschließender Stakeholderanalyse haben sich die mitwirkenden Partner auf das etablierte Datenformat OWL (Web Ontology Language) geeinigt und gitlab als geeignete Plattform zur gemeinsamen Entwicklung und Implementierung identifiziert. Das gitlab wurde von der IT des ika zur Verfügung gestellt und wird seitdem aktiv genutzt.

Die Arbeiten wurden mit einer Literaturrecherche zum Thema Ontologien im Allgemeinen und Verkehrsontologien im Speziellen begonnen.

Ontologie Literaturrecherche

Besonders relevante Titel sind **fett** markiert.

Allgemeines zu Ontologien

Autoren	Titel	Link	Relevanz
Horridge et al.	**A Practical Guide To Building OWL Ontologies Using Protégé 4 and CO-ODE Tools Edition 1.3**	1	Einführung in OWL-Ontologien, detaillierte Beschreibung der Konzepte und Modellierungsmöglichkeiten
Bergman	Ontology Best Practices	2	Zusammenstellung von Best Practices eines erfahrenen Entwicklers

McGuiness	Ontology Development 101: A Guide to Creating Your First Ontology	3	Ähnlich zu [1], allerdings weniger spezifisch für Protégé

Tabelle 2: Allgemeine Literatur zu Ontologien

Terminologie

Autoren	Titel	Link	Relevanz
Schuldt	Ein Beitrag für den methodischen Test von automatisierten Fahrfunktionen mit Hilfe von virtuellen Umgebungen	1	Definiert Begriffe in den Bereichen des Testens, Straßenaufbaus und der Szenarien
Ulbrich et al.	**Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving**	2	Definiert Begriffe Szene, Situation, Szenario.
Weber et al.	**A Framework for Definition of Logical Scenarios for Safety Assurance of Automated Driving**	3	Darstellung von Szenarien, aufbauend auf 6-Ebenen-Ontologie
Baier et al.	**Richtlinien für die Anlage von Stadtstraßen - RASt 06**	4	Grundlegende Konzepte und Begriffe in der Stadtstraßenplanung

Tabelle 3: Terminologien im Bereich ADS

Ontologien in der Automobildomäne

Autoren	Titel	Link	Relevanz
Bagschik et al.	**Ontology based Scene Creation for the Development of Automated Vehicles**	1	Erzeugung von Szenen aus der 6-Ebenen-Ontologie
Lilis et al.	Personalizing HMI elements in ADAS using ontology meta-models and rule based reasoning	2	Darstellung von Umwelt, Kontext und Fahrern in einer ADAS-Ontologie
Fernandez et al.	Ontology-Based Architecture for Intelligent Transportation Systems Using a Traffic Sensor Network	3	Darstellung von Fahrzeugen, Infrastruktur und Sensorik in einer Ontologie
Lashkov et al.	Ontology-Based Approach and Implementation of ADAS System	4	Darstellung von Fahrzeugen (Sensorik, Trajektorien, Gefährdungen und Straßen)

	for Mobile Device Use While Driving		und Verhalten (Fahrercharakteristika und -profile) in einer ADAS-Ontologie
Boudra et al.	Architecture and Ontological Modelling for Assisted Driving and Interaction	5	Darstellung von Fahrzeugen, Straßen, Verhalten und Kontexten in einer Ontologie
Mohammad et al.	**Ontology-based Framework for Risk Assessment in Road Scenes Using Videos**	6	Darstellung von Risiken (bezogen auf Objekte, Straßen und Umgebungen) in einer Ontologie. Klassifizierung von Risiken mit Hilfe der Ontologie.
Zhao et al.	**Core ontologies for safe autonomous driving**	7	Darstellung von Straßennetzen, Verhalten und Fahrzeugen in einer ADAS-Ontologie.
Zhao et al.	An Ontology-Based Intelligent Speed Adaptation System for Autonomous Cars	8	Implementierung eines ADAS basierend auf Regeln der Ontologie aus [7].
Zhao et al.	Ontologies for Advanced Driver Assistance Systems	9	Detailliertere Vorstellung der Ontologie aus [7].
Armand et al.	**Ontology-Based Context Awareness for Driving Assistance Systems**	10	Darstellung von Objekten und Kontext in einer ADAS-Ontologie. Der abgeleitete Kontext wird u.a. zur Risikoeinschätzung genutzt.
Hülsen et al.	**Traffic intersection situation description ontology for advanced driver assistance**	11	Darstellung von Kreuzungen und Verkehrssituationen in einer ADAS-Ontologie.
Feld et al.	The Automotive Ontology: Managing Knowledge Inside the Vehicle and Sharing it Between Cars	12	Darstellung von Verkehrsteilnehmern, Kontext, Zeitaspekten und Positionierungen in einer ADAS-Ontologie.
Kannan et al.	An Intelligent Driver Assistance System (I-DAS) for Vehicle Safety Modelling using Ontology Approach	13	Darstellung von Fahrzeugen und Kontext in einer ADAS-Ontologie.
Fuchs et al.	**A Model for Ontology-Based Scene Description for Context-Aware Driver Assistance Systems**	14	Darstellung von Verkehrssituationen und -kontexten in einer Ontologie.

Czarnecki	**Operational World Model Ontology for Automated Driving Systems - Part 1: Road Structure**	15	Hohe Ähnlichkeit zur VVM-Ontologie, Fokus hier aber auf der Taxonomie und Abbildung der konkreten, realen Welt, spezifisch für die USA. Definitiv ein guter Aufsatzpunkt für die Taxonomie in VVM.
Czarnecki	**Operational World Model Ontology for Automated Driving Systems - Part 2: Road Users, Animals, Other Obstacles, and Environmental Conditions**	16	s. o.

Tabelle 4: Ontologien aus der Automobildomäne

Basierend darauf wurde ein Architektur-Vorschlag vom DLR (ehem. OFFIS) ausgearbeitet und die Draft Version für die Ontologie als OWL-Datei initial aufgesetzt. Zur reibungslosen Zusammenarbeit wurde ein vom ika vorgeschlagener Workflow speziell für das Ontologie Core-Team etabliert. Darauf aufbauen wurde von PROSTEP ein Review-Prozess für ganz TP2 erstellt, welcher seit dem genutzt wird um Ergebnisse TP2-intern zu reviewen. Weiterhin wurden die verschiedenen Use Cases der Ontologie vom DLR (ehem. OFFIS) identifiziert und strukturiert dokumentiert.

Use Cases der Automotive Urban Traffic Ontology

Die Automotive Urban Traffic Ontology (A.U.T.O.) stellt Artefakte und Phänomene des urbanen Verkehrs dar.

Darstellung von Verkehrswelten

Anwender der Ontologie: Durchführende einer V&V für automatisierte Fahrzeuge, Entwickelnde von V&V-Methoden, Entwickelnde automatisierter Fahrfunktionen

Beschreibung des Falls: Darstellung von u.a. Szenen, Szenarien, Situationen, d.h. der Verkehrswelt und ihren Geschehnissen. Hierbei sollen alle relevanten (abhängig von der jeweiligen Anwendung der Ontologie) Phänomene und ihre Relationen zueinander abgebildet sein. Es ist nicht ausgeschlossen, dass sich noch weitere Konzepte zur Strukturierung der Verkehrswelt entwickeln. Auch diese sollen ontologisch abbildbar sein.

Besondere Fälle:

1. **Szenarienbeschreibung**. *Es besteht eine enge Verbindung zwischen A.U.T.O. und der in AP2.1 entwickelten (abstrakten) Szenarienbeschreibung. Hier kann A.U.TO. dazu dienen (quasi-statische) Teile von Szenarien zu beschreiben, sowie (sehr abstrakte, diskrete) dynamische Teile (bspw. Manöver).*

2. **Abstraktion**. *A.U.T.O. soll genutzt werden, um Abstraktionen von Artefakten und Geschehnissen der Verkehrswelt durchzuführen. Abstraktion ist notwendig zur endlichen Darstellung der Verkehrswelt und entsteht durch Anwendung von Expertenwissen, welches zwingend digital festgehalten werden muss um Nachvollziehbarkeit und Reproduzierbarkeit der Abstraktionsstufen zu gewährleisten.*

Zusammenhang mit anderen Ontologie Use Cases: Eine Repräsentation der Umwelt des automatisierten Fahrzeugs kann anschließend unterstützend zur Identifikation kritischer ontologischer Weltartefakte (Kritikalitätsphänomene) genutzt werden (UC2.1).

Beispiele: Folgende Verkehrsumstände sollen ontologisch beschrieben werden.

1. **Szene.** *Es existieren zwei Fahrzeuge auf zwei Spuren, wobei Fahrzeug 1 hinter Fahrzeug 2 fährt. Beide Spuren haben eine Breite von 2 bis 2,5 Metern. Die Umgebung der Fahrspuren beinhaltet einen Bürgersteig auf jeder Seite, der mit einem Bord zur Straße abgetrennt ist. Weiterhin säumen Gebäude mit Glasfassaden die Straße.*

2. **Situation.** *Für Fahrzeug 1 in obiger Szene ist Fahrzeug 2 in bestimmten Konstellationen von ausgezeichneter Bedeutung, da es die Führung von Fahrzeug 1 möglicherweise davon abhalten kann, sein Ziel (bspw. ein Mobilitäts- oder Performanceziel) unter Berücksichtigung eines bestimmten Wertesystems (Kollisionsvermeidung, Regelbeachtung, …) zu erreichen. Weiterhin interpretiert Fahrzeug 1 den Bürgersteig als unbefahrbares Terrain in der aktuellen Situation. Möglicherweise wird Fahrzeug 1 den Bürgersteig aber in darauffolgenden Situationen befahren müssen.*

3. **Abstraktion.** *Beschreibung der Welten, in denen besonders gefährdete Verkehrsteilnehmer in Kreuzungssituationen vorkommen, bei denen ein Teil der kreuzungsregelnden Verkehrsinfrastruktur ausgefallen ist und ein stark verringerter Reibwert vorliegt.*

Festhalten von Expertenwissen der Domäne „Urbaner Verkehr“

Anwender der Ontologie: Experten der Domäne „Urbaner Verkehr“ und Arbeitsgruppe Ontologie

Beschreibung des Falls: Domänenexperten können mit Hilfe von A.U.T.O. ihr Fachwissen über Verkehrsgeschehen und -struktur digital festhalten. Alternativ kann bereits anderweitig festgehaltenes Fachwissen (bspw. in Form von schriftlichen Richtlinien und Gesetzen) durch die Arbeitsgruppe in A.U.T.O. übertragen werden. Insbesondere sollen auch durch Experten identifizierte Kritikalitätsphänomene, Wirkzusammenhänge und dazugehörige Abstraktionen festgehalten werden können.

Zusammenhang mit anderen Ontologie Use Cases: Das nun ontologisch festgehaltene Fachwissen kann zur Darstellung von Verkehrswelten (UC1.1) und der Anwendung der Kritikalitätsanalyse (UC2.1) genutzt werden.

Beispiele: Folgendes Wissen soll ontologisch festgehalten werden.

1. **Richtlinien.** *Regelquerschnitte und Richtlinien zur Anlage von Stadtstraßen sollen digital festgehalten werden. Das Expertenwissen zu möglichen Anordnungen von Fahrbahnelementen, wie bspw. Breiten und Kurvenradien, ist in textuellen Richtlinien festgehalten. Dies wird nun durch die Arbeitsgruppe Ontologie axiomatisch in A.U.T.O. eingetragen.*

2. **Abstraktion.** *Während der Kritikalitätsanalyse identifiziert ein Experte, dass sowohl Radfahrer als auch Fußgänger in gewissen Fällen zur Klasse der „besonders gefährdeten Verkehrsteilnehmern“ abstrahiert werden können.*

Sprache zum Annotieren von Verkehrsdaten

Anwender der Ontologie: Ausführende der Annotation von Verkehrsdaten

Beschreibung des Falls: In VVMethoden sollen eingefahrene Szenarien annotiert werden. Dazu existiert in AP2.1 der Arbeitspunkt der „Szenarienannotation“. A.U.T.O. kann hierfür die zugrundeliegende Fachsprache über Verkehrsobjekte und -relationen zur Verfügung stellen.

Zusammenhang mit anderen Ontologie Use Cases: Wenn annotierte Szenarien sich an die ontologisch festgelegte Fachsprache halten, können die Annotationen auf Grund der Kompatibilität ohne Mehraufwand in eine ontologische Datenbank aufgenommen werden (UC2.2)

Beispiel*: In einem eingefahrenen Szenario mit einem PKW und einem Radfahrer sollen die Verkehrsteilnehmer und ihre Beziehungen zueinander annotiert werden. Die Begriffe der Klassen („Personenkraftwagen“, „Radfahrer“) und der Relationen („Distanz zwischen Verkehrsteilnehmern“), die zur Annotation genutzt werden, stammen aus A.U.T.O.*

Use Cases der VVM-Ontologie

Die VVM-Ontologie stellt im Projekt diskutierte und entworfene Konzepte der Verifikation und Validierung von hochautomatisierten Fahrzeugen dar. Sie inkludiert die Automotive Urban Traffic Ontology, so dass hier über Konzepte der Verkehrswelt argumentiert werden kann.

Werkzeug in der Kritikalitätsanalyse

Anwender der Ontologie: Entwickler und Anwender der Kritikalitätsanalyse

Beschreibung des Falls: In der Kritikalitätsanalyse wird über Phänomene der Verkehrswelt und ihre Relationen untereinander argumentiert. Die VVM-Ontologie bietet der Kritikalitätsanalyse einen zentralen Ort, an dem diese Phänomene sowohl für Menschen lesbar als auch für Maschinen interpretierbar festgehalten sind. Die VVM-Ontologie hält in der Kritikalitätsanalyse identifizierte Wirkzusammenhänge und Kritikalitätsphänomene und ihre Relationen zu eben diesen festgehaltenen Artefakten der Verkehrswelt fest. Weiterhin dient sie in der Analyse als Werkzeug zur wissensbasierten Abstraktion von Kritikalitätsphänomenen und Wirkzusammenhängen. Außerdem unterstützt die VVM-Ontologie die Bildung von Szenarienklassen, ein wichtiger Schritt in der Kritikalitätsanalyse, über die festgehaltenen Abstraktionen und ihre Verbindung zur Szenarienbeschreibung.

Zusammenhang mit anderen Ontologie Use Cases: Die Kritikalitätsphänomene und Wirkzusammenhänge werden über Artefakte und Phänomene der Verkehrswelt und ihren Relationen untereinander beschrieben (UC1.1). Weiterhin werden Szenarienklassen über die abstrakte Szenarienbeschreibung gebildet (UC1.1-1). Die Abstraktionen erfolgen unter anderem wissensbasiert (UC1.1-2, UC1.2).

Beispiele: In der Kritikalitätsanalyse kann die VVM-Ontologie wie folgt genutzt werden.

1. **Kritikalitätsphänomene.** *Während einer Iteration der Analyse wird identifiziert, dass das ontologisch festgehaltene Phänomen „Niedrige Temperatur“ mit erhöhter Unfallwahrscheinlichkeit und -schwere korreliert. Es wird daher als Kritikalitätsphänomen digital in der VVM-Ontologie festgehalten, mit Referenz auf das in UC1.1/1.2 gefundene und dargestellte Phänomen „Temperatur“.*

2. **Wirkzusammenhänge.** *Die darauffolgende Kausalitätsanalyse identifiziert folgende plausible Kausalzusammenhänge zwischen dem Phänomen „Niedrige Temperatur“ und Kritikalität: Niedrige Temperatur führt zu einer höheren Wahrscheinlichkeit, dass die Straße vereist ist („Eis auf der Straße existiert“). Durch Eis auf der Straße verringert sich der Reibwert. Durch den verringerten Reibwert verlängert sich der Bremsweg und die laterale Steuerbarkeit der Fahrzeuge nimmt ab. Dadurch entstehen schwer kontrollierbare Situationen, die die Kritikalität erhöhen. Dieser Wirkzusammenhang wird nun ontologisch festgehalten, indem die Relationen zwischen den Artefakten „Temperatur“, „Straße“, „Eis“, „Reibwert“, „Fahrzeug-Bremsweg“, „Fahrzeug-laterale Steuerbarkeit“, „Kontrollierbarkeit“, „Kritikalität“ eingetragen werden. Weiterhin wurde im Plausibilisierungsschritt herausgefunden, dass der Wirkzusammenhang nicht bei fehlendem Wasser auf der Straße gilt. Der Wirkzusammenhang wird ontologisch angepasst festgehalten: „Niedrige Temperatur UND Wasser auf der Straßenoberfläche sind notwendig für Eis auf der Straße“.*

3. **Szenarienklassen.** *Über die abstrakte Szenarienbeschreibung können nun mit Hilfe der VVM-Ontologie alle Szenarien beschrieben werden, die die Eigenschaften des oben beschriebenen Wirkzusammenhangs erfüllen. Beispielsweise. soll unter anderem der Zusammenhang der Phänomene „Wasser auf Straße UND niedrige Temperatur“ in allen Szenen der Szenarien der Klasse vorhanden sein. In einem Abstraktionsschritt wird diese Klasse von Szenarien möglicherweise mit anderen Klassen zusammengelegt: Es werden nur noch Szenarien betrachtet, die das abstrakte Phänomen „Glätte“ beinhalten, welches vorher von Experten in der VVM-Ontologie festgehalten wurde. Über das Wissen in der VVM-Ontologie lernen wir während der Analyse auch, welche Verbindung zwischen „Glätte“ und den anderen Phänomenen im Wirkzusammenhang existiert (bspw. impliziert „Glätte“ einen verringerten Reibwert, der aber durch Benutzung von Schneeketten mitigiert werden kann).*

Deklaration von Wissens- und Datenbanken in VVM

Anwender der Ontologie: Entwickler und Nutzer von Datenbanken

Beschreibung des Falls: Das Datenbankschema der sogenannten Entwicklungsdatenbank kann als über die in der VVM-Ontologie festgehaltenen Entitäten und Relationen realisiert werden (bspw. in einer relationalen Datenbank oder Graphdatenbank). Beispielsweise kann das Wissen über Kritikalitätsphänomene und Wirkzusammenhänge digital abgelegt werden. Queries an die Datenbank können mit Querysprachen für Ontologien (bspw. SPARQL) realisiert werden, sofern das Datenbankschema kompatibel mit der VVM-Ontologie ist. Dies ermöglicht über die in der VVM-Ontologie festgehaltene Semantik eine semantische Suche in Datenbanken. Weiterhin können abzuspeichernde Daten auf Konsistenz bezüglich der in der VVM-Ontologie festgehaltenen Axiome untersucht werden (Reasoner). Ein Anwendungsfall einer Wissensbank wurde bereits in UC1.2 beschrieben. Allgemeiner kann auch abseits der Domäne „Verkehr“ Fachwissen in der Wissensbank festgehalten werden, beispielsweise über das Testen von L4/L5-Fahrzeugen.

Zusammenhang mit anderen Ontologie Use Cases: Da Verkehrswelten über A.U.T.O. modelliert werden können (UC1.1), sind alle Instanzen dieser Welten, die sich an das in der VVM-Ontologie spezifizierte Schema halten, in einer entsprechenden Graphdatenbank speicherbar. Hierfür inkludiert die VVM-Ontologie A.U.T.O., es können aber auch Konzepte außerhalb von A.U.T.O. in der Datenbank festgehalten werden (bspw. Kritikalitätsphänomene). Das Expertenwissen liefert Relationen die zur Konsistenzanalyse genutzt werden können (UC1.2). Eine

solche Datenbank von Instanzen von Verkehrswelten unterstützt die Kritikalitätsanalyse (UC2.1), da die gleiche Sprache sowohl für die Speicherung von Daten als auch für die Analyse genutzt wird.

Beispiele:

1. **Datenbankschema**. *Das Abspeichern eines konkreten Szenarios mit zwei Fahrzeugen F1 und F2. Über die VVM-Ontologie ist bekannt, dass jedes Fahrzeug eine Geschwindigkeit und eine Position (x, y) hat. Daher werden F1 und F2 mit den Informationen v_F1 = 100 km/h und v_F2 = 120 km/h und pos_F1 = (0, 1) und pos_F2 = (10, 2) abgespeichert.*

2. **Semantische Suche**. *Beispielhafter Query: Finde alle Szenarien mit zweispurigen Kreuzungen, in denen zwei valide platzierte PKWs mit geringem Abstand und hoher Relativgeschwindigkeit zueinander existieren.*

Kommunikationsmittel in VVMethoden & V&V-Domänensprache

Anwender der Ontologie: Projektpartner in VVMethoden und V&V-Experten

Beschreibung des Falls: Dem Datenfluss im Projekt liegt die VVM-Ontologie zu Grunde. Daher sollten essentielle Bestandteile des Projektdatenflusses, sofern technisch umsetzbar, in der VVM-Ontologie abgebildet sein. Entsprechende Konzepte aus der Domäne der Verifikation & Validierung finden ihren Platz in der VVM-Ontologie, und erlauben im Projekt einheitlich über diese Konzepte zu argumentieren.

Zusammenhang mit anderen Ontologie Use Cases: Eng verwandt mit UC2.4, da über die Fachsprache im Projekt kommuniziert werden soll.

Beispiele:

1. **Fahrauftrag.** *TP2 gibt einen Fahrauftrag an TP6 weiter. Die im Fahrauftrag spezifizierten Bedingungen sind in der VVM-Ontologie festgehalten. TP6 kann ihre Bedeutung in der VVM-Ontologie nachschlagen.*

2. **Testfallspezifikation.** *TP4 spezifiziert Anforderungen an Testfälle. Die Elemente der Tests und ihre Bedeutung sind in der VVM-Ontologie festgehalten, so dass TP7 ein angemessenes Testvorgehen ableiten kann.*

Begriffsregister

Anwender der Ontologie: Projektpartner in VVMethoden

Beschreibung des Falls: In AP1.6 wird ein Begriffsregister erstellt, welches alle für das Projekt relevanten Begriffe und ihre Definitionen enthält. Zu diesen muss im Projekt ein Konsens über ihre Bedeutung erreicht werden. Im TP3 wurde eine Begriffsmethodik erstellt, um systematisch solche Bedeutungen abzuleiten. Die gefundenen Definitionen und die in der Methodik identifizierten Relationen zu anderen Konzepten (z.B. Kontext, Subjekt, Objekt, Abgrenzung) werden auch in der VVM-Ontologie festgehalten.

Zusammenhang mit anderen Ontologie Use Cases: Das Festhalten des Begriffsregisters in der VVM-Ontologie ermöglicht eine konsistente Projektkommunikation (UC2.3).

Beispiel: *Der Begriff des „Testfalls“ soll aus dem Begriffsregister in die VVM-Ontologie überführt werden. Hierfür wird die Definition in der VVM-Ontologie als Kommentar annotiert, und die Relation zwischen anderen Objekten festgehalten (bspw. Testspezifikation und Testergebnis). Weiterhin kann der Kontext beschrieben werden (Testfall ist im Kontext der V&V von automatisierten Fahrfunktionen zu verstehen).*

Schließlich wurde erhöhter Diskussionsbedarf beim urbanen 6-Ebenen-Modell, welches als wichtiger Teil der VVM-Ontologie das PEGASUS 6-Ebenen-Modell erweitern soll, festgestellt. Diese Diskussion ist nicht Teil von Kapitel 3.1.2.2.2.1 E2.1a - Draft Version Ontologie, sondern wird im Folgeergebnis 3.1.2.2.2.2 E2.1b - Relevante Kernkonzepte in der Ontologie vollständig beschrieben entsprechend weitergeführt.

3.1.2.2.2.2 E2.1b - Relevante Kernkonzepte in der Ontologie vollständig beschrieben

Es wurde zuerst ein nicht-formaler Entwurf und eine Architektur für die Ontologie erarbeitet, die anschließend in OWL umgesetzt wurde. Die Entwicklung gliedert sich grob in folgende Abschnitte:

> **Architektur**, beschreibt den groben Aufbau und die Konzeption von A.U.T.O., die in den folgenden drei Abschnitten ausdetailliert wird:
>
> 1. **Metamodell** für die Instanziierung der Verkehrsentitäten in Szenen und Szenarien
> 2. **Verkehrsverwandte Konzepte**: Darstellung genutzter Ontologien
> 3. **Verkehrsentitäten**: Cores & Implementierungen der einzelnen Ebenen des 6-Ebenen-Modells (Fokus auf Ebenen 5, 4 und 1).

Architektur

Für das vorherige Ergebnis E2.1a wurden Ontologie Use Cases aufgestellt. Darauf basierend wurden die Architektur von A.U.T.O. abgeleitet, welche sich in drei Kernaspekte gliedert:

1. **Verkehrsmodelle**
2. **Verkehrsverwandte Konzepte**
3. **Verkehrsentitäten**, beschrieben mit Hilfe des 6-Ebenen-Modells

Verkehrsentitäten beschreiben die in der Verkehrswelt existierenden Dinge, bspw. Verkehrsteilnehmer und deren Manöver. Verkehrsmodelle aggregieren eine Menge von **Verkehrsentitäten** dann zeitlich über bspw. Szenen oder Szenarien. Konzepte, die nicht direkt Teil der Verkehrswelt sind, aber notwendig für die Beschreibung dieser sind (bspw. geometrische Konzepte), sind aus dem 6-Ebenen-Modell als **verkehrsverwandte Konzepte** ausgelagert. Bildlich dargestellt:

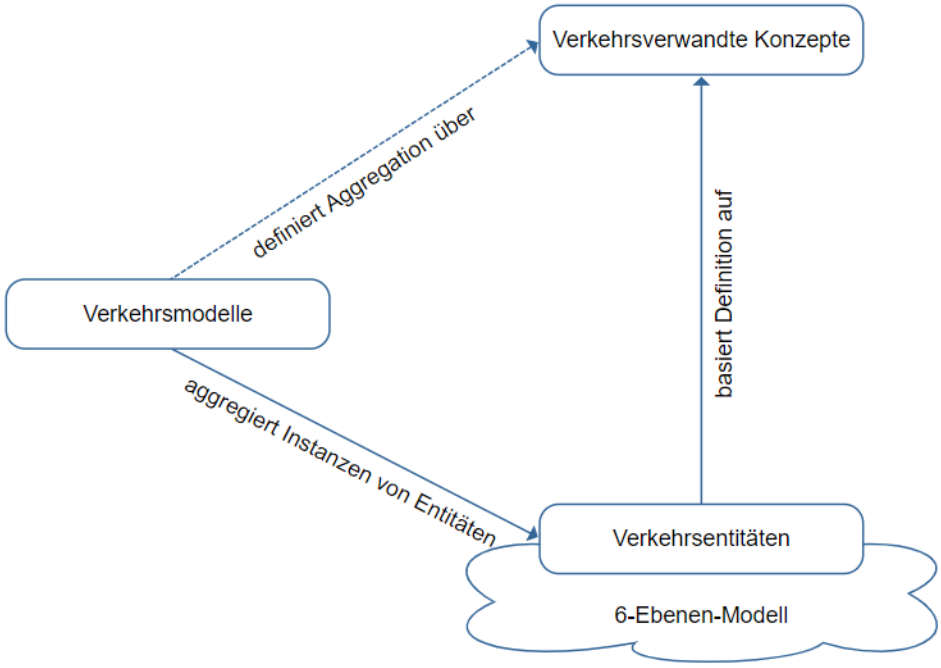


Abbildung 161: Kernaspekte der A.U.T.O.-Architektur.

Basierend auf dieser Dreiteilung wurde folgende Architektur erarbeitet:

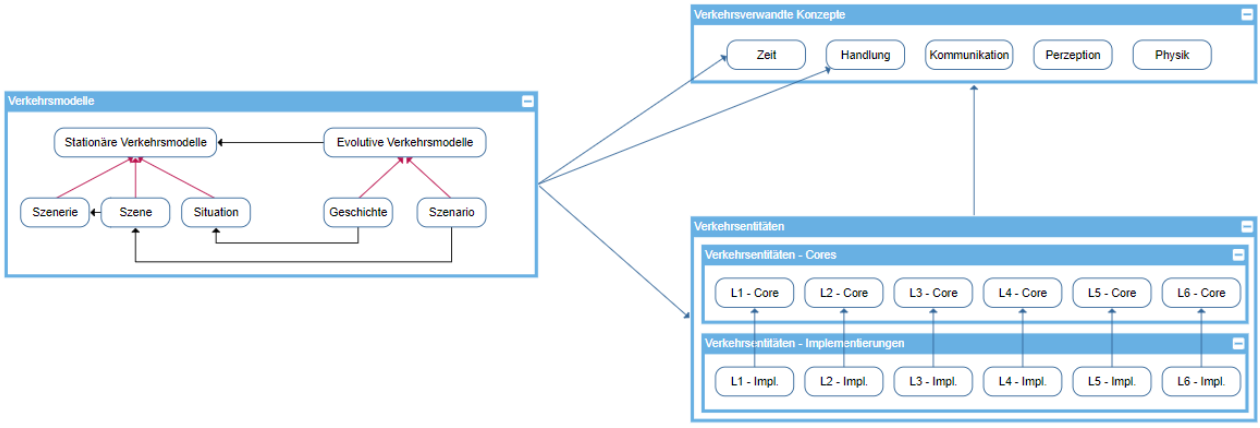


Abbildung 162: A.U.T.O.-Architektur

Zusammenfassung der Ergebnisse:

- Gemeinsame Veröffentlichung zum urbanen 6-Ebenen-Modell: 6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment
- Gemeinsame Veröffentlichung zu A.U.T.O.: Using Ontologies for the Formalization and Recognition of Criticality for Automated Driving
- Veröffentlichung der Ontologie auf GitHub unter MIT-Lizenz:
    - Ontologie: https://github.com/lu-w/auto

- Tooling: https://github.com/lu-w/criticality-recognition

3.1.2.2.2.3 E2.1c - Verfeinerung Semantik der Szenarienannotation

Das Ergebnis E2.1c ist im Wesentlichen der Konferenzbeitrag Holistic Driving Scenario Concept for Urban Traffic.

Szenariobasierte Ansätze sind für die Verifizierung und Validierung von automatisierten Fahrsystemen aufgrund der Komplexität des Verkehrs wichtig, welche durch Tests auf der Straße nicht abgedeckt werden kann. Eine Herausforderung ist die Definition eines Szenarienkatalogs, der nicht zu abstrakt ist, um dieser Komplexität gerecht zu werden, aber dennoch eine überschaubare Anzahl von Fahrszenarien enthält. In diesem Beitrag wird ein semi-formaler Ansatz zur Ableitung eines Szenarienkatalogs vorgestellt, der zu weniger als 300 Basisszenarien führt, die in einer Fahrszenario-Datenbank für die Sicherheitsvalidierung des automatisierten Fahrens verwendet werden sollen. Der Ansatz definiert abstrakte Konzepte als Sammlungen von Merkmalen zur Unterscheidung verschiedener Fahrszenarien. Innerhalb der High-Level-Kategorien werden bestimmte Konzepte kombiniert, entweder als vollständige Faktorisierung von Merkmalen oder durch die Berücksichtigung, dass die Kombination von Merkmalen andere Merkmale impliziert. Es werden auch Oberklassen definiert, um Szenarien mit gemeinsamen Merkmalen zu gruppieren. Der Ansatz bildet Interaktionen in der realen Welt effizient ab und kann viele bestehende Kataloge innerhalb vordefinierter Grenzen abdecken.

3.1.2.2.3 AP2.2 - Ermittlung von kritikalitätsbeeinflussenden Wirkzusammenhängen und Szenarienerzeugung

3.1.2.2.3.1 E2.2a - Kritikalitätsanalyse für ein dynamisches Phänomen (Verdeckung) auf bestehender Datenbasis und Analyse der Ergebnisse

Parallel zur Entwicklung der Methode "Kritikalitätsanalyse" wird diese exemplarisch für das Kritikalitätsphänomen 'Verdeckung' durchgeführt. Das Dokument zur Gesamtmethodik beschreibt umfassend alle Methodenbausteine und illustriert diese für 'Verdeckung'. Für den wissens-getriebenen Teil der Kritikalitätsanalyse wurden zunächst expertenbasiert Kritikalitätsphänomene identifiziert und strukturiert festgehalten. Für den empirischen Teil der Kritikalitätsanalyse wurde dabei initial die GIDAS-Datenbank hinsichtlich des Phänomens 'Verdeckung' analysiert. Dies geschah im Zuge der Zusammenarbeit mit der VUFO (GUA4) im Rahmen der AG Knotenpunkt-Unfälle.

Beides kann unter Identifikation von Kritikalitätsphänomenen & Wirkzusammenhängen zusammengefasst werden. Zukünftige Iterationen erweitern insbesondere den empirischen Teil um weitere Datenquellen.

Evasion Threat Metrics (ETM)

Motivation

Seitens der Gesellschaft besteht die Forderung, die Verletzungswahrscheinlichkeit im Straßenverkehr deutlich zu verringern. Deshalb ist die Entwicklung einer Kritikalitätsmetrik, die die Verletzungswahrscheinlichkeit mit physikalischen Größen der Fahrzeugbewegung in Beziehung setzt, von großer Bedeutung.

Vorgehensweise

Man prädiziert die Bewegungen des Ego-Fahrzeugs und des anderen Verkehrsteilnehmers unter Berücksichtigung realistischer Stellerdynamik und definiert zwei Submetriken, die alternierend eingesetzt werden, siehe Abbildung 163.

- Solange die Kollision noch vermeidbar ist, wird der minimale Abstand d_{min} des anderen Verkehrsteilnehmers vom Ego-Fahrzeug als Submetrik verwendet.
- Ist die Kollision nicht mehr vermeidbar, dann dient die Verletzungswahrscheinlichkeit als Submetrik.

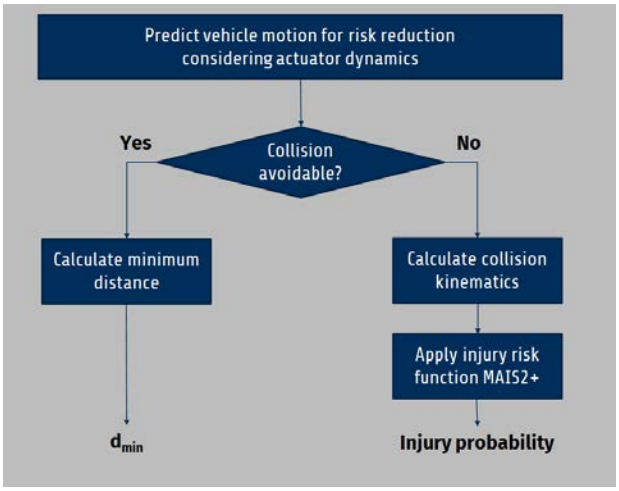


Abbildung 163: Flussdiagramm für die Berechnung der ETM

Injury Risk Functions

Injury Risk Funktionen setzen die Verletzungswahrscheinlichkeit mit Fahrzeugbewegungsgrößen wie z. B. der Geschwindigkeitsdifferenz vor - nach der Kollision in Beziehung. In Zusammenarbeit von ZF, VW und dem Bosch Unfallforschungsteam wurden Injury Risk Funktionen für die Kollisionspaarungen Fahrzeug-Fußgänger, Fahrzeug-Radfahrer und Fahrzeug-Fahrzeug entwickelt.

Diagramme

Die Abbildung 164 zeigt die beiden ETM Diagramme:

- Das ax-ay Diagramm spannt den Optionsraum für Unfallvermeidung durch kombiniertes Bremsen und Lenken auf.
- Das Zeitdiagramm zeigt die Entwicklung der Metriken über der Zeit. Dargestellt werden die negativen Werte von d_{min} und die positiven Werte der Verletzungswahrscheinlichkeit, die stetig an die Werte von $-d_{min}$ am Nulldurchgang anschließen.

In den gezeigten Diagrammen wird ein Fahrzeug-Fahrzeug Auffahrunfall analysiert.

Das ax-ay-Diagramm zeigt, dass das Ego-Fahrzeug die Möglichkeit hat, die Kollision durch Bremsen oder Lenken oder Kombinationen davon zu vermeiden.

Die Abbildung 164 rechts zeigt die Annäherung des Ego-Fahrzeugs ohne Lenken und Bremsen. Das Zeitdiagramm startet mit einer vermeidbaren Kollision, was durch $-d_{min} < 0$ (blaue Linie) angezeigt wird. Wenn $-d_{min}$ die Nulllinie erreicht, wird die Kollision unvermeidbar, und die Verletzungswahrscheinlichkeiten (rote Linien) für die Person im Ego-Fahrzeug und in dem anderen Fahrzeug steigen auf Werte größer als 0.

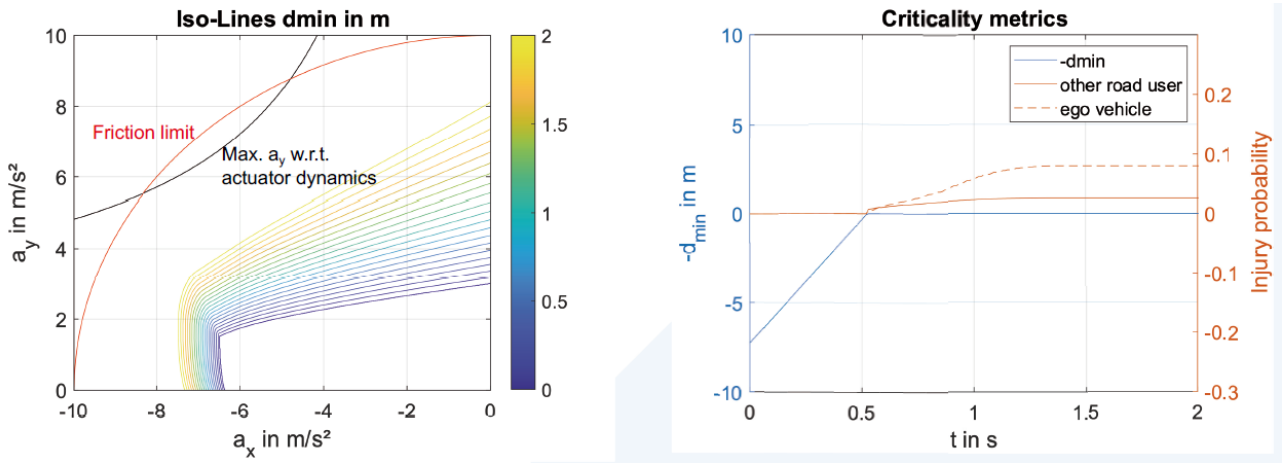


Abbildung 164: Links: ax-ay Diagramm mit Höhenlinien von d_{min}, rechts: Zeitliche Entwicklung der Kritikalitätsmetriken

Nutzen der ETM

Die ETM ist ein neuer Satz von Kritikalitätsmetriken,

- die ein gesellschaftliches Ziel (Reduktion der Verletzungsschwere) mit physikalischen Größen (Fahrzeugbewegungsgrößen) in Verbindung bringen,
- die eine Analyse von kombiniertem Bremsen und Lenken ermöglichen,
- die für Fahrzeug-Fußgänger, Fahrzeug-Radfahrer und Fahrzeug-Fahrzeug Szenarien verfügbar sind.

Zonen Graphen – Eine topologische Abstraktion zur Beschreibung und Analyse von Verkehrssituationen in der SOCA Analyse

Die Analyse von Verkehrssituationen ist ein notwendiger Schritt bei der **Zerlegung** der **Operating Domain**. **Zonengraphen** sind eine **topologische Abstraktion** von geometrischen Bereichen innerhalb einer Verkehrslandschaft, die für das situative Fahren relevant sind. Ein Zonengraph besteht aus verschiedenen Zonentypen:

- Fahrzonen für das AV,
- Positionszonen für andere Verkehrsteilnehmer,
- Informationszonen.

Der Weg des AV durch die Fahrzonen wird durch die Intentionskanten vorgegeben. Bedrohungskanten verknüpfen Positionszonen mit den Fahrzonen. Informationskanten verbinden Informationszonen mit den Fahrzonen. In der nachfolgenden Abbildung ist oben eine schematische Skizze eines Zonengraphen für einen Fußgängerübergang an einer T-Kreuzung für

den Funktionalen UseCase "Straight Passing of a T-Crossing with Pedestrian Crossing" dargestellt. Darunter eine geometrische Realisierung für eine konkrete T-Kreuzung basierend auf einer OpenDrive Karte sowie dem topologischen Zonengraph dargestellt.

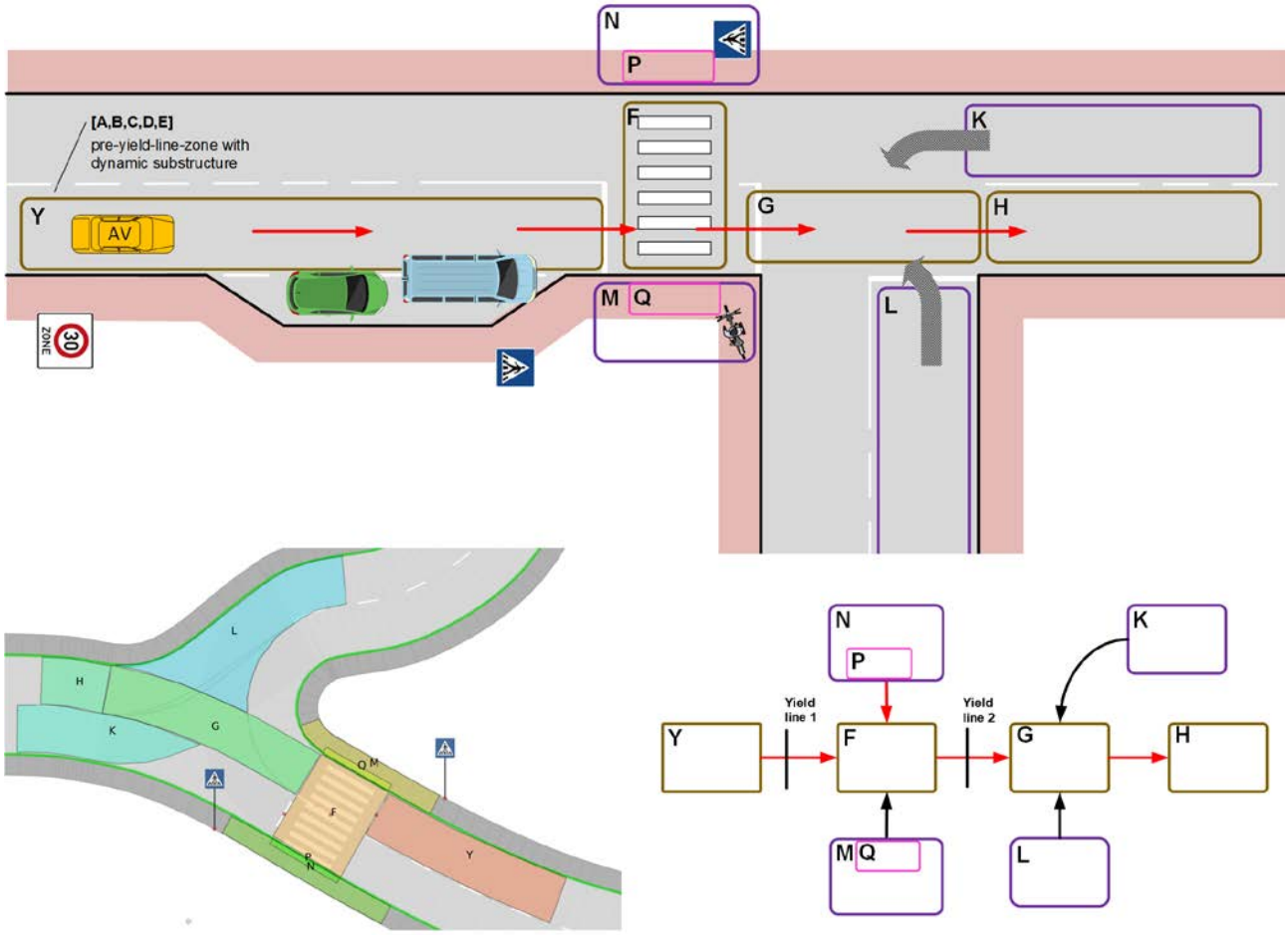


Abbildung 165: Schematische Skizze eines Zonengraphen für einen Fußgängerübergang an einer T-Kreuzung und geometrische Realisierung mit topologischem Zonengraph

Diese Abstraktion reduziert die Komplexität der Darstellung und unterstützt dadurch unter anderem bei der Strukturierung einer Semantischen Analyse oder einer Gefahren- und Risikoanalyse (HARA).

SOCA – SCODE 4 Open Context Analysis

SOCA (Scode for Open Context Analysis) wurde für zwei Hauptanwendungsbereiche entwickelt [92]:

Erstens zielt SOCA darauf ab, das extern beobachtbare Verhalten des Systems zu analysieren. Auf dieser Ebene macht SOCA keine Annahmen darüber, wie das ADS tatsächlich implementiert wird oder wie es die Welt um sich herum wahrnimmt. Zweitens kann mit SOCA gezielt die Entscheidungslogik eines (regelbasierten) Verhaltensplaners oder die notwendigen abstrakten Szenarien zum Testen (welcher Art auch immer) eines Verhaltensplaners analysiert werden.

Da die reale Welt eine riesige, wenn nicht unendliche, Vielfalt an Verkehrssituationen bietet, die potenziell vom ADS gemeistert werden müssen, müssen wir geeignete Abstraktionen für den Umgang mit Verkehrssituationen einführen. Dazu verwendet SOCA zwei Konzepte: Zonengraphen

für eine geometrische Abstraktion und eine morphologische Verhaltensanalyse, um Äquivalenzklassen basierend auf dem geforderten Verhalten des ADS abzuleiten. Diese auf der SCODE-Methode basierende morphologische Analyse ermöglicht eine Vollständigkeitsprüfung der abgeleiteten Äquivalenzklassen in Bezug auf den in der Analyse verwendeten Entscheidungsraum. Diese beiden Komponenten ergeben ein Modell, das eine Reihe von kontextabhängigen Anforderungen auf Systemebene bereitstellen kann. Darüber hinaus kann das Modell verwendet werden, um einen geeigneten Satz von Szenarien für das Testen abzuleiten.

SOCA verwendet Zonengraphen, die von konkreten Straßengeometrien und konkreter Bevölkerung mit Objekten und anderen Verkehrsteilnehmern abstrahieren. Für jede Art von Landschaft, z. B. eine 4-Wege-Kreuzung, einen einzelnen Fußgängerübergang oder eine mehrspurige Straße, wird für jede ADS-Absicht ein Zonengraph erstellt. Wenn wir zum Beispiel eine 4-Wege-Kreuzung betrachten, erstellen wir Zonengraphen, einen für die Linkskurve, einen für die Rechtskurve und einen für die Geradeausfahrt, wenn wir nur diese drei Absichten berücksichtigen. Der Zonengraph ist eine topologische Abstraktion des tatsächlichen Layouts (wie Straßenwinkel, Krümmung, Spurbreite, ...).

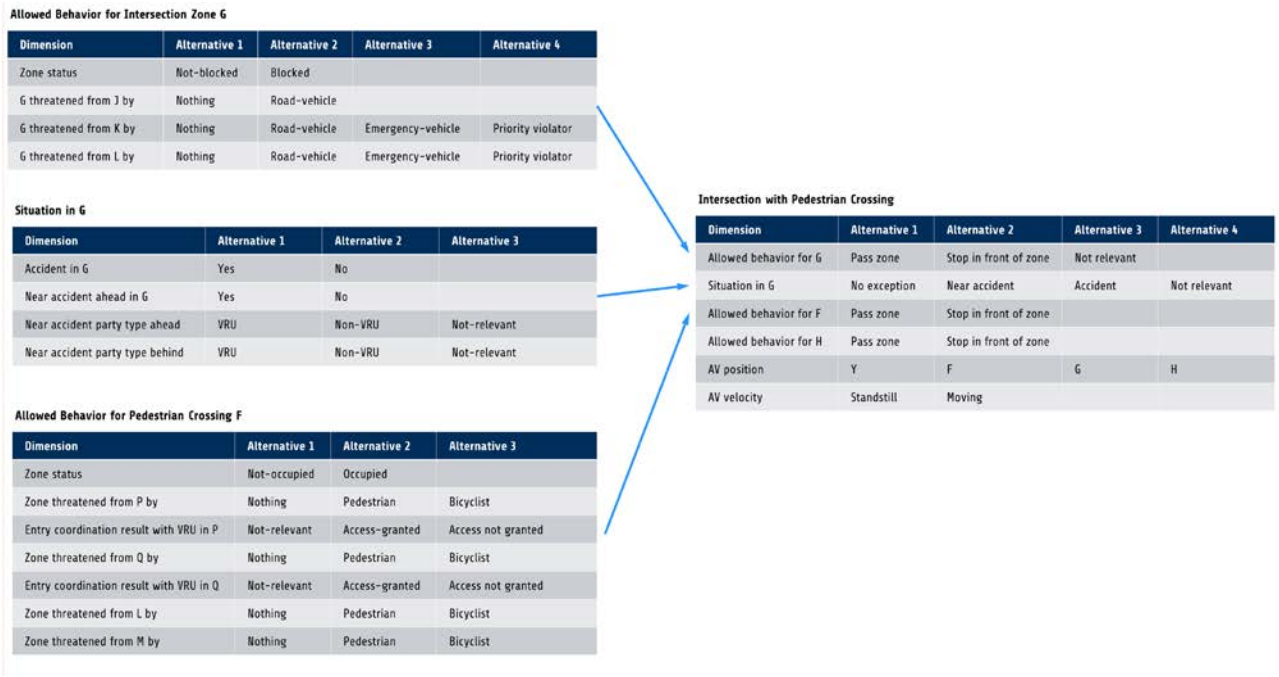
Fahrzonen und Positionszonen können individuell mit unterschiedlichen Verkehrsteilnehmern belegt werden. Zonen werden im Allgemeinen durch die Notwendigkeit definiert, zwischen verschiedenen Bedingungen zu unterscheiden, die notwendig sind, um über das Verhalten des Fahrzeugs zu entscheiden. Es gibt auch eine natürliche 'Vererbung' über diese drei Arten. Jede Fahrzone ist natürlich auch eine Positionszone für andere Verkehrsteilnehmer. Jede Positionszone ist eine Informationszone in dem Sinne, dass wir Informationen aus dieser Zone benötigen, z. B. von einem anderen Verkehrsteilnehmer besetzt wird.

Die Integration einer Ontologie (wie oben beschrieben) für die automatische Besetzung von Zonen ist hier sinnvoll ist und erhöht die Genauigkeit der verwendeten Terme.

Eine Zone wird im topologischen Sinne während einer SOCA-Analyse verwendet. Der Fahrweg ist in eine Liste von Fahrzonen aufgeteilt. Jeder Split wird durch einen anderen Satz von Bedingungen motiviert, die verwendet werden, um das gewünschte Verhalten anzugeben.

Ausgehend von der Darstellung der Kreuzung erstellen wir zunächst eine erste Zwicky Box, um SCODE zur Ableitung des Verhaltens anzuwenden. Eine Zwicky-Box oder morphologische Box ist eine Darstellung eines diskreten Raumes, der durch das kartesische Produkt der Dimensionen gegeben wird. Jede Dimension stellt einen Informationsaspekt des Systemkontextes dar, der für Entscheidungen und das Verhalten des entsprechenden Systems relevant sein kann und durch eine endliche Menge paarweiser disjunkter Alternativen besteht. Äquivalenzklassen werden durch Kombinationen einer oder mehrerer Alternativen für jede Dimension definiert.

Mit dieser Zwicky-Box können wir nun die Äquivalenzklassen für das Verhalten definieren. Die Analyse ist abgeschlossen, wenn der Entscheidungsraum vollständig von den Äquivalenzklassen abgedeckt ist und die Äquivalenzklassen konsistent sind, d.h. keine Überschneidungen aufweisen. Etwas formeller bedeutet Vollständigkeit, dass jede Kombination, die im Entscheidungsraum existiert, mindestens einer Äquivalenzklasse hinzugefügt wurde. Konsistenz bedeutet, dass jede Kombination aus dem Entscheidungsraum zu höchstens einer Äquivalenzklasse hinzugefügt wurde. Für jede der Fahrzonenzustand-Dimensionen wird eine separate zusätzliche Analyse durchgeführt, um die Bedingungen abzuleiten, wann sie passierbar" oder nicht passierbar" sind. Insbesondere kann hier eine Analyse für mehrere Fahrzonen verwendet werden.



Allowed Behavior for Intersection Zone G

Dimension	Alternative 1	Alternative 2	Alternative 3	Alternative 4
Zone status	Not-blocked	Blocked		
G threatened from J by	Nothing	Road-vehicle		
G threatened from K by	Nothing	Road-vehicle	Emergency-vehicle	Priority violator
G threatened from L by	Nothing	Road-vehicle	Emergency-vehicle	Priority violator

Situation in G

Dimension	Alternative 1	Alternative 2	Alternative 3
Accident in G	Yes	No	
Near accident ahead in G	Yes	No	
Near accident party type ahead	VRU	Non-VRU	Not-relevant
Near accident party type behind	VRU	Non-VRU	Not-relevant

Allowed Behavior for Pedestrian Crossing F

Dimension	Alternative 1	Alternative 2	Alternative 3
Zone status	Not-occupied	Occupied	
Zone threatened from P by	Nothing	Pedestrian	Bicyclist
Entry coordination result with VRU in P	Not-relevant	Access-granted	Access not granted
Zone threatened from Q by	Nothing	Pedestrian	Bicyclist
Entry coordination result with VRU in Q	Not-relevant	Access-granted	Access not granted
Zone threatened from L by	Nothing	Pedestrian	Bicyclist
Zone threatened from M by	Nothing	Pedestrian	Bicyclist

Intersection with Pedestrian Crossing

Dimension	Alternative 1	Alternative 2	Alternative 3	Alternative 4
Allowed behavior for G	Pass zone	Stop in front of zone	Not relevant	
Situation in G	No exception	Near accident	Accident	Not relevant
Allowed behavior for F	Pass zone	Stop in front of zone		
Allowed behavior for H	Pass zone	Stop in front of zone		
AV position	Y	F	G	H
AV velocity	Standstill	Moving		

Abbildung 166: Zwicky-Box für einen beispielhaften Entscheidungsraum

Von Situationen zum Szenario

Für viele der Downstream Methoden wird oft nicht die situative Sichtweise von SOCA genutzt, sondern Szenarien sich die sich auf Abläufe fokussieren. Da ein Szenario als eine Abfolge von Situationen verstanden werden kann, können die genannten Bedingungen für die Beschreibung von Restriktionen für ein Szenario genutzt werden. Mithilfe einer zeitlichen Beschreibung (z. B. basierend auf regulären Ausdrücken oder einer zeitlichen Logik) können die Restriktionen als Teil einer **abstrakten Szenariobeschreibung** genutzt verstanden werden. Eine graphische Darstellung eines solchen Szenarios für den skizzierten UseCase kann dann zum Beispiel so aussehen:

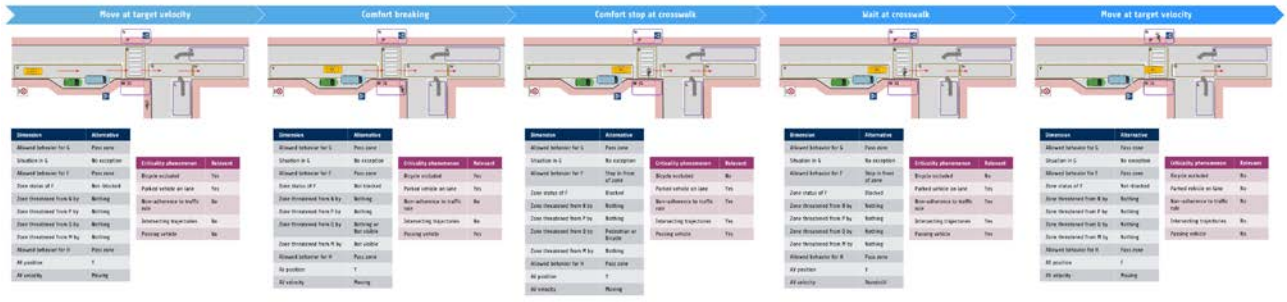


Abbildung 167: Szenario in Form einer Abfolge von externen Bedingungen

Die Grafik zeigt ein Szenario in Form einer Abfolge von externen Bedingungen, welche auf einem gewünschten Fahrverhalten gründen, basierend auf unserem Modell. Das Szenario entwickelt sich von links nach rechts. Die blauen Tabellen unten zeigen eine Auswahl aktueller Alternativen auf dem Entscheidungsraum. Die roten Tabellen zeigen die Verknüpfung des Modells und der Szenarioentwicklungen mit den relevanten Kritikalitätsphänomenen in der jeweiligen Szene.

3.1.2.2.3.2 E2.2b - Konzept für generische Systematik der Kritikalitätsbetrachtung

Das Ergebnis E2.2 beinhaltet die Ausarbeitung eines Konzepts der Methode "Kritikalitätsanalyse". Diese Ausarbeitung erfolgte im Zuge der Erstellung des Deliverables D01 und ist im entsprechenden Dokument ausführlich dargelegt. Eine weiterentwickelte und ausführlichere Version ist als Journalpapier bei IEEE Access veröffentlicht.

3.1.2.2.3.3 E2.2c - in E2.2a überführt

3.1.2.2.3.4 E2.2d - Generische Systematik der Kritikalitätsbetrachtung mit weitestgehender Abdeckung

Für das Ergebnis E2.2d wurde das initiale Konzept der Kritikalitätsanalyse weiterentwickelt und die exemplarische Durchführung der Kritikalitätsanalyse im urbanen Raum auf eine breitere Basis gestellt. Dies bedeutet daher eine Weiterentwicklung von E2.2b und Deliverable D01. Folgende Ergebnisse wurden hier erarbeitet:

- Journal Publikation Leveraging the GIDAS Database for the Criticality Analysis for Automated Driving Systems: Identifikation von Kritikalitätsphänomen in der GIDAS Datenbank in Zusammenarbeit mit VUFO und VW im Rahmen des GUA4, Analyse der resultieren Case-Phenomenon Relation Matrix, Berechnung von mit Kritikalitätsphänomenen assoziierten Risiken auf Basis der Analyse.
- Masterarbeit Application of Evolutionary Algorithms to Analyze Criticality in Urban Traffic Scenarios: Instanziierung und Evaluierung von logischen Szenarienklassen basierend auf den Functional Use Cases in CARLA unter Nutzung von Evolutionären Algorithmen mit innovativen Kritikalitätsmetriken als Zielfunktion.
- Masterarbeit Towards threat metric evaluation in complex urban scenarios: Untersuchung von Kritikalitätsmetriken auf dem inD-Datensatz mit Hilfe von Erreichbarkeitsberechnungen, sowie Konformitätsuntersuchungen von Akteurmodellen, mit Fahrspurberücksichtigung.
- Journal Publikation Criticality Metrics for Automated Driving: A Review and Suitability Analysis of the State of the Art: extensives Review-Papier zu Kritikalitätsmetriken sowie Einführung einer Methode 'Suitability Analysis' zur anforderungsgetriebenen Auswahl von Kritikalitätsmetriken für verschiedene Anwendungsfälle des automatisierten Fahrens.
- Zusammenfassung der Ergebnisse im Deliverable D08: Generische Systematik der Kritikalitätsbetrachtung.

3.1.2.2.3.5 E2.2e - Identifikation kritikalitätserhöhender Verkehrsphänomene

E2.2e ist das finale Ergebnis der exemplarischen Umsetzung des Prozessschritts "Identifikation von Kritikalitätsphänomenen", der Kritikalitätsanalyse für die Domäne "Urban" in VVMethoden.

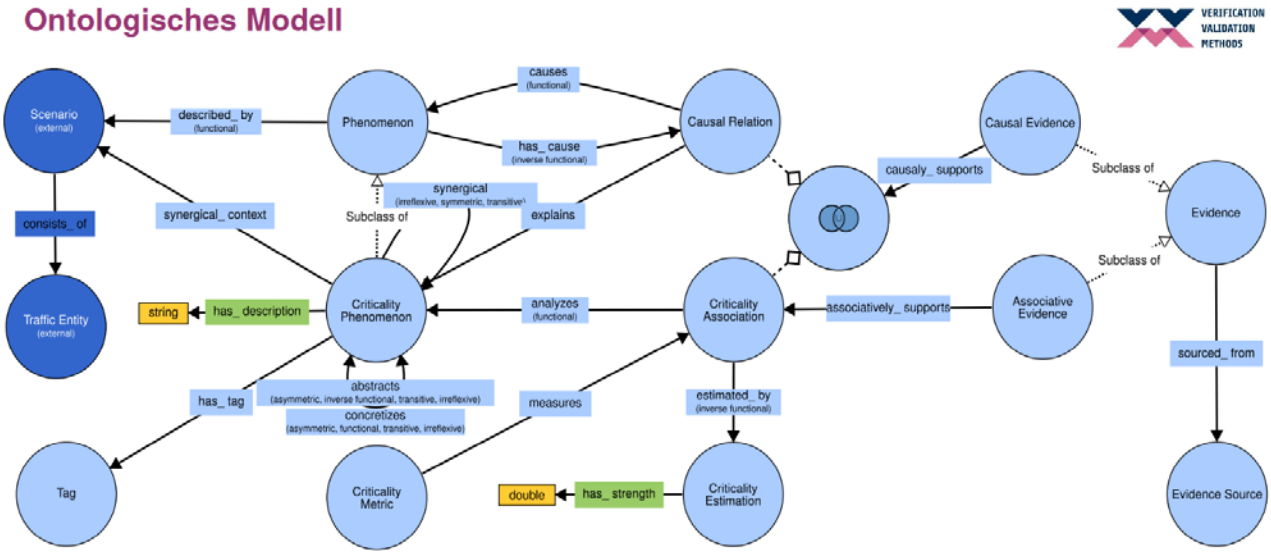


Abbildung: Ontologisches Modell der Entität 'Kritikalitätsphänomen' und ihrer Relationen visualisiert in VOWL

Abbildung 168: Ontologisches Modell der Entität „Kritikalitätsphänomen“ und ihrer Relationen visualisiert in VOWL

Die Liste der Kritikalitätsphänomene (Excel) wurde von v1.7 (für GIDAS-Analyse) zu einer v2.0 erweitert, in der das Konzept Perfekte vs. Reale Technologie aus E2.4a eingearbeitet wurde. Die v2.0 ist jedoch unvollständig und wurde nicht weiter geführt sondern in eine Graphdatenbank überführt, siehe auch D08: Generische Systematik der Kritikalitätsbetrachtung. Insbesondere wurden Sensorphänomene, also Kritikalitätsphänomene basierend auf Perzeption aus AP2.4, ab v2.0 hinzugefügt und ergänzt.

Die Hauptergebnisse von E2.2e sind somit die Kritikalitätsphänomen-Datenbank (neo4j), das zugehörige Handbuch und der Export als owl-Datei.

3.1.2.2.3.6 E2.2f - Definition der Anforderungen an die Simulation zur Kritikalitätsanalyse

Dieses Ergebnis beinhaltet verschiedene Anwendungsfälle der Simulation in der Kritikalitätsanalyse und die daraus resultierende Sammlung aller Anforderungen an die Simulation zur Kritikalitätsanalyse die das VVMethoden TP2 in der Projektlaufzeit erhoben. Des Weiteren werden auch die entsprechenden Methoden vorgestellt auf welchen die systematische Ableitung solcher Anforderungen basiert.

Ergebnisse:

- Anwendungen von Simulation in der Kritikalitätsanalyse: Skizzierung von Anwendungsfällen der Simulation in der Kritikalitätsanalyse & Illustration anhand von Beispielen
- Mindestanforderungen an openPASS für Kritikalitätsanalyse anhand Functional Use Cases
- Die "Mindestanforderungen an openPASS für Kritikalitätsanalyse" wurden zu Beginn des Projekts anhand der Functional Use Cases, d.h. Szenario-basiert, auf dem Level von funktionalen urbanen Szenarien vom TP2 erhoben und in Absprache mit TP5 und SET Level abgeglichen und auf dessen Realisierbarkeit geprüft. Die Umsetzung der realisierbaren Anforderungen, d.h. Weiterentwicklungen an openPASS zur

Kritikalitätsanalyse wurden im Rahmen des GUA5 gemeinsam mit TÜV Süd und in-tech kontinuierlich umgesetzt und auch teilweise bereits in die öffentliche Version von openPASS integriert.

- Weiterhin wurden im TP2, basierend auf Kritikalitätsphänomenen, exemplarisch Anforderungen an Sensormodelle für die Simulation abgeleitet (für Kamera & Lidar). Hierbei wurde insbesondere zwischen phänomenologischen und physik-basierten Sensormodellen unterschieden.

- Im Papier Grasping Causality for the Explanation of Criticality for Automated Driving (Zum Zeitpunkt der Erstellung dieses Berichts in Begutachtung beim Journal ACM Transactions on Intelligent Systems and Technology) wird die in der Kritikalitätsanalyse vorgesehene Kausalanalyse von Kritikalitätsphänomenen basierend auf Pearl's Kausaltheorie eingeführt. Insbesondere in Abschnitt 5.2 wird dort auf Anforderungen an Simulationsumgebungen eingegangen, welche aus der Verwendung von Kausalmodellen resultieren.

- Zusammenfassung der Ergebnisse im Deliverable D09: Anforderungen an die Simulation zur Kritikalitätsanalyse

3.1.2.2.3.7 E2.2g - Wesentliche Phänomene für den betrachteten Raum analysiert

Der Traum vom autonomen Fahren könnte durch die fortschreitende Technologie der letzten Jahrzehnte schnell verwirklicht werden. Die Akzeptanz dieser Technologie in der Gesellschaft und bei Zulassungsbehörden führt jedoch schnell zu der Forderung nach einer Sicherheitsargumentation. Das Ausmaß dieser Sicherheit wird gerne an menschlichen Fähigkeiten festgemacht und relativiert sich mit der Aussage, dass ein autonomes Fahrzeug oder eine autonome Fahrintelligenz besser fahren soll als ein Mensch. Daraus ergibt sich die Herausforderung: Wie kann die Sicherheit oder besser die Qualität einer Fahrintelligenz bewertet werden? Im Folgenden dient die Fahrintelligenz als Sammelbegriff für alle Objekte, die ein Fahrzeug steuern, egal ob menschlich oder digital. Eine Bewertung der Fahrintelligenz nur anhand der Anzahl der Unfälle wäre als Ansatz zu trivial, schließlich können auch Beinahe-Unfälle ein starkes Indiz für eine geringe Fahrintelligenz sein. Um dieses Spannungsfeld quantitativ zu beschreiben, wurde als beschreibende Größe die Kritikalität gewählt, also die Wahrscheinlichkeit, dass im weiteren Verlauf eines Szenarios ein Unfall eintritt.

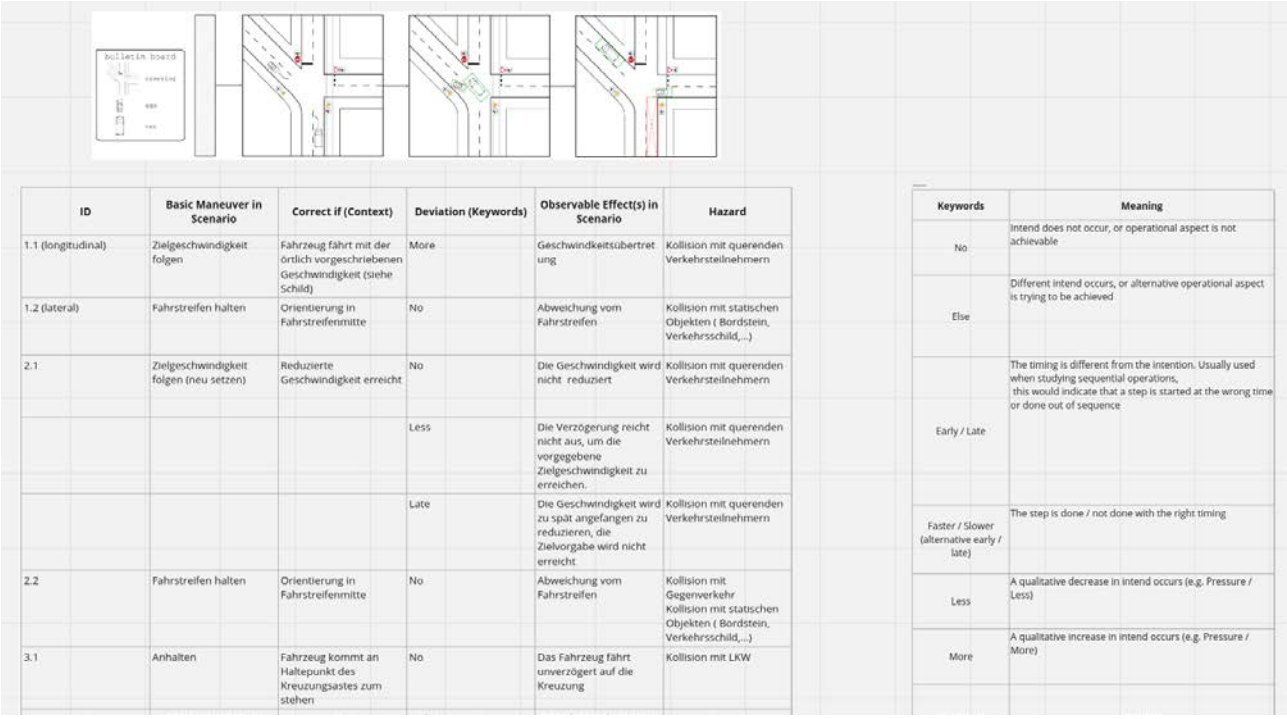
In diesem Ergebnis werden ausgewählte Kritikalitätsmetriken mit Hilfe von Design of Experiments (DoE) und Sensitivitätsanalysen quantitativ verglichen. Die im VVM-Projekt definierten funktionalen Anwendungsfälle werden in einem sinnvollen, logischen Parameterraum variiert und in einer Simulationsumgebung ausgeführt. Die resultierenden konkreten Trajektorien werden mit dem Tool CriSys ausgewertet und quantitativ im Parameterraum verglichen. Abschließend sprechen wir Empfehlungen für ein Kritikalitätslevel für jeden Functional Use Case aus, basierend auf den Resultaten des quantitativen Vergleichs.

3.1.2.2.4 AP2.3 - Sicherheitsprinzipien und Gesamtmethodik Kritikalitätsanalyse

3.1.2.2.4.1 E2.3a - Initiale Gefährdungsanalyse für Use Case Szenarien

Die Gefährdungsanalyse für die Functional Use Cases wurde in VVMethoden als Querschnittsthema zwischen TP2 und TP3 identifiziert und fällt somit in den Bereich der AG Core01 - Open-Context Integration. Im Rahmen der AG Core01 wurden von Nayel Fabian Salem (TU Braunschweig) & Christian Lalitsch-Schneider (ZF) eine mehrteilige, kollaborative Reihe von

Workshops organisiert und vorbereitet. Während in den Workshops Nr.1 und Nr. 2 die Zonierung von Szenen/Szenarien und die Bestimmung des Soll-Verhaltens im Vordergrund stand, wurde im Workshop Nr.3 die Gefährdungsanalyse fokussiert.



ID	Basic Maneuver in Scenario	Correct if (Context)	Deviation (Keywords)	Observable Effect(s) in Scenario	Hazard
1.1 (longitudinal)	Zielgeschwindigkeit folgen	Fahrzeug fährt mit der örtlich vorgeschriebenen Geschwindigkeit (siehe Schild)	More	Geschwindkeitsübertretung	Kollision mit querenden Verkehrsteilnehmern
1.2 (lateral)	Fahrstreifen halten	Orientierung in Fahrstreifenmitte	No	Abweichung vom Fahrstreifen	Kollision mit statischen Objekten (Bordstein, Verkehrsschild,...)
2.1	Zielgeschwindigkeit folgen (neu setzen)	Reduzierte Geschwindigkeit erreicht	No	Die Geschwindigkeit wird nicht reduziert	Kollision mit querenden Verkehrsteilnehmern
			Less	Die Verzögerung reicht nicht aus, um die vorgegebene Zielgeschwindigkeit zu erreichen.	Kollision mit querenden Verkehrsteilnehmern
			Late	Die Geschwindigkeit wird zu spät angefangen zu reduzieren, die Zielvorgabe wird nicht erreicht	Kollision mit querenden Verkehrsteilnehmern
2.2	Fahrstreifen halten	Orientierung in Fahrstreifenmitte	No	Abweichung vom Fahrstreifen	Kollision mit Gegenverkehr Kollision mit statischen Objekten (Bordstein, Verkehrsschild,...)
3.1	Anhalten	Fahrzeug kommt an Haltepunkt des Kreuzungsastes zum stehen	No	Das Fahrzeug fährt unverzögert auf die Kreuzung	Kollision mit LKW

Keywords	Meaning
No	Intend does not occur, or operational aspect is not achievable
Else	Different intend occurs, or alternative operational aspect is trying to be achieved
Early / Late	The timing is different from the intention. Usually used when studying sequential operations, this would indicate that a step is started at the wrong time or done out of sequence
Faster / Slower (alternative early / late)	The step is done / not done with the right timing
Less	A qualitative decrease in intend occurs (e.g. Pressure / Less)
More	A qualitative increase in intend occurs (e.g. Pressure / More)

Hier wurden durch Anwendung einer modifizierten, Schlüsselword-getriebenen HAZOP, basierend auf Kramer et al., Gefährdungen für das automatisierte Fahrzeug auf Fahrzeugebene identifiziert. Insbesondere wurden betrachtet FUC2-3 – Occlusion of Bicyclist through Parking Cars sowie FUC3-1 – Traffic with Right of Way. Die Ergebnisse werden nun als Input für AP3.2 – Lokale Sicherheitsbetrachtung weiterverwendet.

3.1.2.2.5 AP2.4 - Ermittlung Güteanforderungen Sensorik

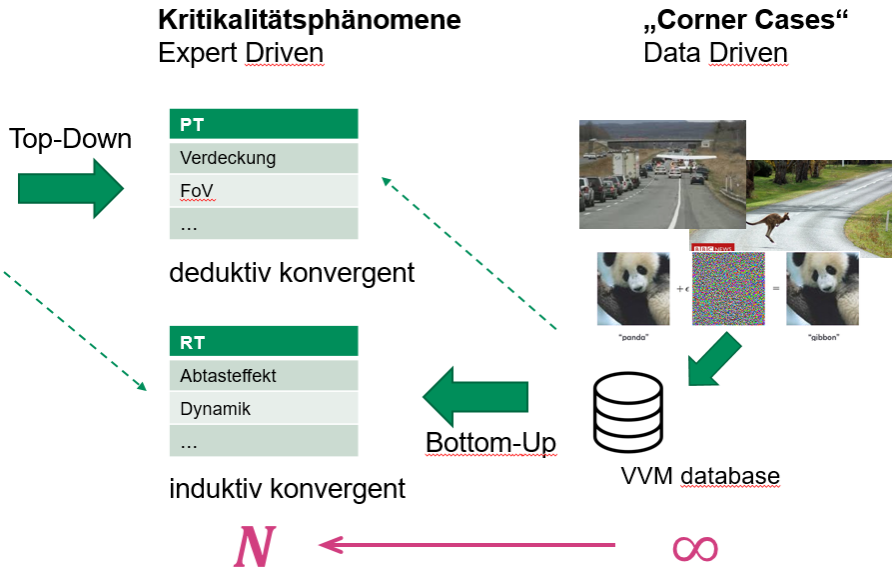
3.1.2.2.5.1 E2.4a - Analyse der Auswirkungen von Perzeptionscharakteristika

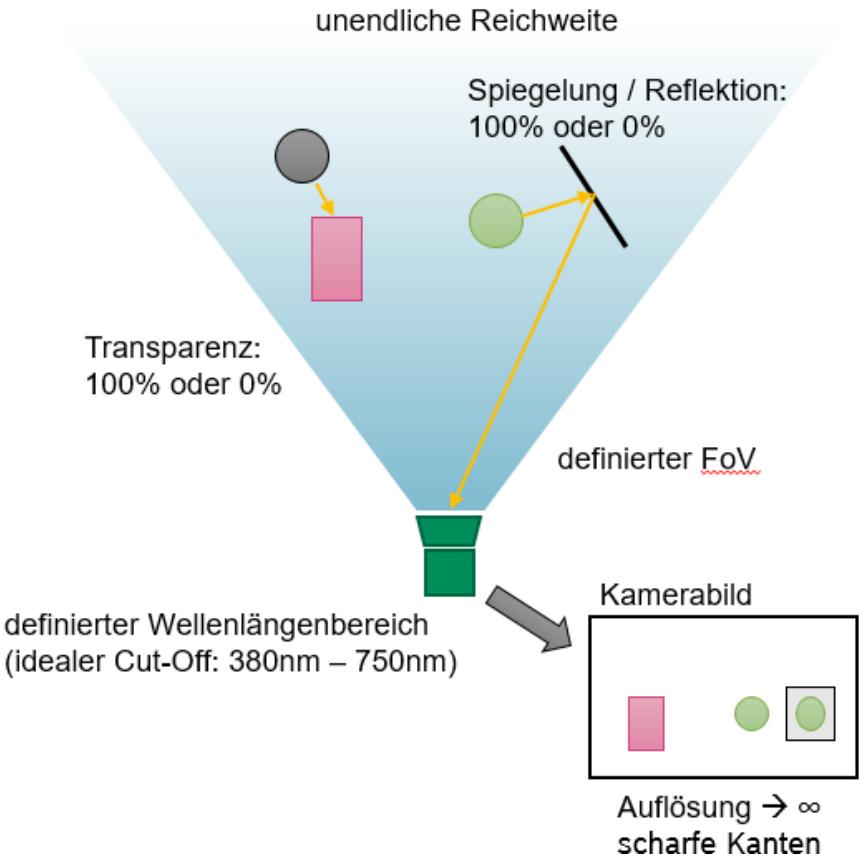
Das erste Projektergebnis des AP2.4 – Ermittlung Güteanforderungen an Sensorik heißt „Analyse der Auswirkungen von Perzeptionscharakteristika“. Das Ergebnis E2.4a setzt sich aus den folgenden Teilergebnissen zusammen:

State of the Art "Leistungsfähigkeit Sensoren": basierend auf der AP2.4 Materialsammlung Perzeption wurde hier die Leistungsfähigkeit des aktuellen Stands der in automatisierten Fahrzeugen verwendeten Sensoren bzgl. verschiedener Kategorien analysiert und bewertet. Das Ergebnis der 'State of the Art' kann zum Abgleich zwischen technologischer Realität und Anforderungen an die Perzeption genutzt werden.

Umfeld-Sensor	Aktiv / Passiv	Horizontale Winkelauflösung (°)	Vertikale Winkelauflösung (°)	Pixelauflösung (MP)	Updaterate (Hz)	FoV Horizontal (Winkel in °)	FoV Vertikal (Winkel in °)	Minimale Reichweite (m)	Maximale Reichweite (m)	Genauigkeit	Kosten	Farberkennung	Abstandsmessung	Geschwindigkeits-messung
Kamera	Typabhängig	10-30 px/°		Typabhängig	20-50	Typabhängig	Typabhängig	Je nach Aufbau	Typabhängig	Niedrig	Typabhängig	Typabhängig	Typabhängig	Nein
Monokamera	Passiv			2-10	20-50	Typabhängig	Typabhängig	Je nach Aufbau	Auflösungsabhängig	Niedrig	Niedrig	Ja	Nein	Nein
Stereokamera	Passiv			2-10	20-50	Typabhängig	Typabhängig	Je nach Aufbau	60 (Zuverlässige Abstandsmessung)	Niedrig	Mittel	Ja	Ungenau	Nein
Topviewkamera (Surround View)	Passiv			2-10	20-50	360			Auflösungsabhängig	Niedrig	Mittel	Ja	Nein	Nein
3D/ToF-Kamera	Aktiv			< 0.08		Typabhängig	Typabhängig	Je nach Aufbau	Auflösungsabhängig	Niedrig	Hoch	Ja	Ja	Nein
Wärmebildkamera	Passiv			< 0.01					150 (abhängig von Intensität)	Niedrig	Mittel	Nein	Nein	Nein
Radar	Aktiv	2-4°		-	10	45-180	5-20	1	30-200	Mittel	Mittel	Nein	Ja	Ja
Short-Range-Radar	Aktiv	2-4°		-	10	180	5-20	1	30	Mittel	Mittel	Nein	Ja	Ja
Mid-Range-Radar	Aktiv	2-4°		-	10	90	5-20	1	100	Mittel	Mittel	Nein	Ja	Ja
Long-Range-Radar	Aktiv	2-4°		-	10	45	5-20	1	200	Mittel	Mittel	Nein	Ja	Ja
Lidar	Aktiv	0,1°-0,4°		-	5-20	180-360	40	<0,1	300	Hoch	Hoch	Nein	Ja	Ja
360 Grad Lidar (Lidar Scanner)	Aktiv	0,1°-0,4°		-	5-20	360	40	<0,1	300	Hoch	Hoch	Nein	Ja	Ja
Optical Phased Array Lidar (Multibeam)	Aktiv	0,1°-0,4°		-	5-20	180	40	<0,1	300	Hoch	Hoch	Nein	Ja	Ja
Ultraschall	Aktiv			-		45			10	Niedrig	Niedrig	Nein	Ja	Ja
Aktives Infrarot	Aktiv			-		30			5	Niedrig	Niedrig	Nein	Ja	Ja

Konzept für reale/perfekte Perzeptionstechnologie: Zur abstrakten Kategorisierung von Kritikalitätsphänomen, welche die Perzeption betreffen (= Perzeptionsphänomene), wurde im AP2.4 ein Konzept für die Unterscheidung zwischen "realer Perzeptionstechnologie" und "perfekter Perzeptionstechnologie" entwickelt. Insbesondere lag hierbei der Fokus auf den Sensoren Kamera, Radar, Lidar sowie dem Perzeptionsalgorithmus. Das Konzept wurde von Roman Gansch (Bosch) auf dem 27. SafeTrans Industrial Day vorgestellt. Das Konzept wird im Detail in Deliverable D08 - Advances on the Criticality Analysis for Automated Driving Systems beschrieben.



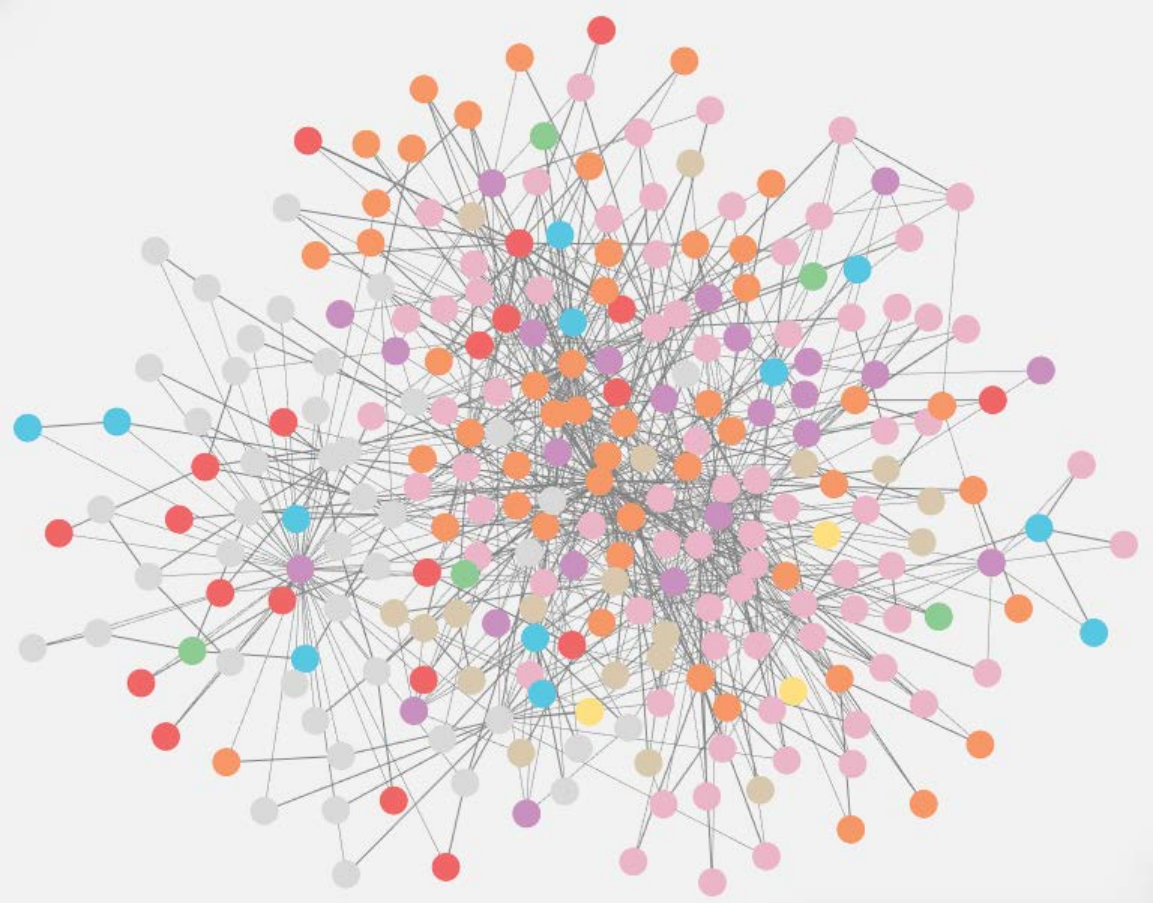


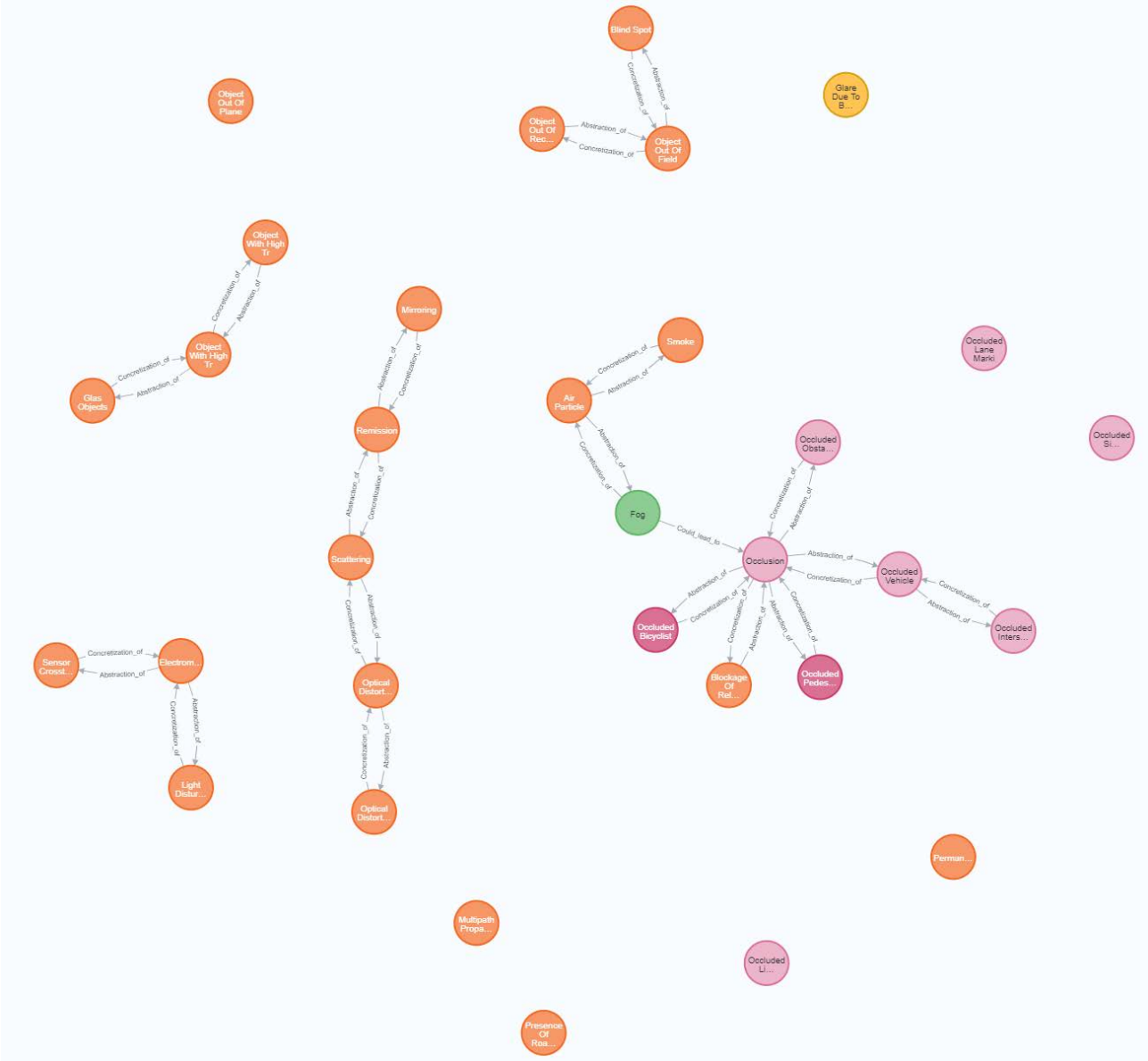
Ergänzung der Kritikalitätsphänomene um Perzeptionsphänomene: die Identifikation von Kritikalitätsphänomenen im AP2.2 – Ermittlung von kritikalitätsbeeinflussenden Wirkzusammenhängen und Szenarienerzeugung wurde konzeptionell in zwei Schritte aufgeteilt:

1) Identifikation von Phänomenen, welche das Fahrzeug/den Verkehr als Ganzes betreffen und nicht perzeptionsspezifisch sind und

2) Identifikation von Perzeptionsphänomenen.

Insbesondere der Schritt 2) hat große inhaltliche Überschneidungen mit AP2.4 und wurde dort auch zu einem großen Teil erarbeitet. Die erweiterte Liste der Kritikalitätsphänomene wurde in eine neo4j-Datenbank überführt, welche unter AP2.2 Kritikalitätsphänomen-Datenbank (neo4j) beschrieben ist. Die Datenbank der Kritikalitätsphänomene wird ebenfalls im Detail im Deliverable D08 - Advances on the Criticality Analysis for Automated Driving Systems beschrieben.





3.1.2.2.5.2 E2.4b - Anforderungen an Perzeption zur Kritikalitätsvermeidung

Das zweite Ergebnis des AP2.4 heißt 'Anforderungen an Perzeption zur Kritikalitätsvermeidung' (E2.4b) und setzt sich aus den folgenden Teilergebnissen zusammen:

1. Methodik zur Analyse der Sollperzeption – hierbei werden aus einer qualitativen Szenarienbeschreibung konkrete Anforderungen an die Perzeption abgeleitet. Die Sollperzeption wird anhand eines Szenarios durch Region-of-Interests (RoI) für jedes ODD-Element und Anforderungen an die Integrität spezifiziert. Input hierfür ist eine Szenarienbeschreibung in TSC / SOCA Format; der Output besteht aus der Geometrie der RoIs für jedes ODD-Element inkl. Integritätsanforderungen.

2. Kausalanalyse von Kritikalitätsphänomenen (hier gibt es eine nicht-leere Schnittmenge mit AP2.2: Erarbeitung der mathematischen Grundlagen für die Kausalanalyse des Effekts von Perzeptionsphänomenen auf geeignete Kritikalitätsmetriken. Auch Ansätze zur Integration von Sicherheitsprinzipen in die Gesamtmethodik der Kritikalitätsanalyse sowie zur Ableitung von Anforderungen an die Datenerhebung zur Plausibilisierung von

Wirkzusammenhängen und für die Wirksamkeit von Sicherheitsprinzipien werden beleuchtet.

3. Kollaborative Ausarbeitung von Perzeptionswirkzusammenhängen für Functional Use Case 1.3 und weitere Perzeptionsphänomene

Im AP2.4 wurde zur Kausalanalyse von Kritikalitätsphänomenen ein Papier 'Grasping Causality for the Explanation of Criticality for Automated Driving' erarbeitet (Zum Zeitpunkt der Erstellung dieses Berichts in Begutachtung beim ACM Transactions on Intelligent Systems and Technology). Es wird vorgeschlagen, den kausalen Einfluss von Einflussfaktoren (SOTIF: „triggering conditions“) auf die gemessene Kritikalität, unter Verwendung von Kritikalitätsmetriken, zu errechnen. Sollte dieser Einfluss hinreichend groß sein, ist es notwendig, ein entsprechendes Sicherheitsprinzip zu entwerfen und auf die (kausale) Effektivität zu untersuchen. Es beinhaltet auch eine Methodik zur Ableitung von Anforderungen an Messdaten, damit eine Kausalinferenz durchgeführt werden kann sowie Sicherheitsprinzipien für Komponenten von automatisierten Fahrsystemen inkl. methodisches Aufzeigen der Messbarkeit der Effektivität von diesen PrinzipienVertiefung von Beispielen mittels Perzeptions-Wirkzusammenhängen für FUC 1.3 & weitere Perzeptionsphänomene (u.a. Occlusion, Multipath Reflection, Field of View, Overhead Structures).

3.1.2.3 TP3 Sicherheitsbewertung und -konzept

Das Teilprojekt 3 hat in VVMethoden im Wesentlichen Beiträge zum Themenfeld "Fähigkeitenanalyse und Verhaltensspezifikation" der Gesamtmethode geleistet. Über die Projektlaufzeit wurden drei Deliverables erstellt, in denen diese Beiträge dokumentiert wurden. Darüber hinaus wurden wissenschaftliche Artikel veröffentlicht, die sich auf den wissenschaftlichen Beitrag der im TP3 konzipierten Methoden und Ansätze fokussieren.

Die im TP3 erzeugten Deliverables sind:

- D02 - Entwurf Systemarchitektur
- D05 - Initiale Quantifizierung der Anforderungen
- D10 - Verbindung globaler und lokaler Argumentationsstrukturen

Aus dem TP3 wurden folgende Arbeiten veröffentlicht:

- N. F. Salem *u. a.*, „Semantische Normverhaltensanalyse zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge“, gehalten auf der 15. Workshop Fahrerassistenz und automatisiertes Fahren, Berkheim, Germany: Uni-DAS e. V., Okt. 2023, S. 95–109. [93]
- N. F. Salem *u. a.*, „Risk Management Core -- Towards an Explicit Representation of Risk in Automated Driving“. arXiv, 15. Februar 2023. doi: 10.48550/arXiv.2302.07715. [76]
- N. F. Salem *u. a.*, „Ein Beitrag zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge“. arXiv, 15. September 2022. doi: 10.48550/arXiv.2209.07204. [71]
- H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach, und J. Reich, „Phenomenon-Signal Model: Formalisation, Graph and Application“. arXiv, 20. Juli 2022. doi: 10.48550/arXiv.2207.09996. [73]

- H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach, und J. Reich, „Phänomen-Signal-Modell: Formalismus, Graph und Anwendung“. arXiv, 31. Juli 2021. doi: 10.48550/arXiv.2108.00252. [72]

In Deliverable 02 wurde der konzeptionelle Grundstein für das Themenfeld "Fähigkeitenanalyse und Verhaltensspezifikation" in VVMethoden gelegt (vgl. Veröffentlichungen oben). Das im Systems Engineering etablierte Konzept der „Fähigkeit“ wurde auf ihren potentiellen Nutzen im Kontext der Absicherung automatisierter Fahrsysteme untersucht (siehe Kapitel 3.1.1.7 Fähigkeitenanalyse und Verhaltensspezifikation). Ergebnis dieser Untersuchung war, dass das Fähigkeitenkonzept insbesondere vor dem Hintergrund konfliktärer Bedürfnisse beteiligter Stakeholder eine Konsolidierung von Bedürfnissen und Anforderungen fördern kann. Zudem wurden Ansätze geschaffen, die es ermöglichen, Systemfähigkeiten auf Basis einer systematischen Beschreibung von Sollverhalten zu formulieren bzw. mögliche Defizite vorhandener Systeme hinsichtlich notwendiger Fähigkeiten zu identifizieren. In Bezug auf die durchgängige Spezifikation und das Design funktionaler Architekturen konnten ebenfalls Beiträge durch die Verwendung des Fähigkeitenkonzepts erarbeitet werden. Während funktionale Architekturen einen festgelegten Blick auf das angestrebte System erfordern, eigenen sich Fähigkeiten zur systemagnostischen Betrachtung eines Systems von Systemen. Bei der Analyse dieses Systems von Systemen steht der Akteur, den das automatisierte Fahrsystem implementiert, im Vordergrund. Durch diese Perspektive ist es möglich, Sollverhalten des Akteurs in Bezug zu seiner operationalen Umgebung zu spezifizieren und dessen Sicherheit zu bewerten (siehe Kapitel 3.1.1.7 Fähigkeitenanalyse und Verhaltensspezifikation).Deliverable 05 baut auf den Erkenntnissen aus Deliverable 02 auf und fokussiert die quantitative Betrachtung von Sollverhalten, Fähigkeiten und Sicherheitsanforderungen. Die Arbeiten an diesem Ziel haben den im TP3 entwickelten Ansatz „Risk Management Core“ hervorgebracht (siehe Kapitel 3.1.1.2 Methodischer Überblick). Der Risk Management Core stellt die Grundlage für eine explizite Repräsentation von Risiken automatisierter Fahrsysteme dar (vgl. [50]). Der Abgleich geschätzter, vom System ausgehender Risiken mit akzeptierten Risiken, welche aus Risikoakzeptanzkriterien abgeleitet werden, führt nach dem Risk Management Core zu einer expliziten Definition von Sicherheitsmaßnahmen inklusive notwendiger Risikominderung und Sicherheitsintegrität. Da der Risk Management Core zunächst ein abstraktes Vorgehen beschreibt, wurde der Ansatz im Zuge des Deliverable 05 auf die Verhaltensspezifikation angewendet. Im Ergebnis wurde ein Vorgehen zur Erstellung eines Verhaltenssicherheitskonzepts konzipiert und exemplarisch umgesetzt. Der übergeordneten Rolle der Sicherheitsargumentation wird in Deliverable 10 Rechnung getragen (siehe Kapitel 3.1.1.2 Methodischer Überblick). Im Deliverable 10 wurde die übergeordnete (globale) Struktur der von VVMethoden vorgeschlagenen Sicherheitsargumentation vorgestellt. Im Fokus stand darüber hinaus die tieferliegende (lokale) Argumentationsstruktur, welche die Beiträge einer durchgängigen Verhaltensspezifikation argumentativ in die Sicherheitsargumentation integriert. Strukturgebende Konzepte der globalen Sicherheitsargumentation sind im Wesentlichen der Risk Management Core sowie die VVMethoden Sicht "Development & Operation | Global". Mit der im Deliverable 10 vorgeschlagenen Argumentation wurde ein argumentativer Ansatz geschaffen, Konformität mit verschiedenen normativen Vorgaben zu begründen und zu belegen. Die in den Deliverables beschriebenen Inhalte sind größtenteils über die oben referenzierten Veröffentlichungen abgedeckt.

3.1.2.4 TP4 Regelwerk System - und Testanforderungen

Übergeordnete Zielsetzung des TP 4 ist die Ableitung eines Regelwerks und Methodik für System- und Testanforderungen am Beispiel urbane Kreuzung, auf deren Basis eine Homologation und Sicherheitsnachweis für das autonome Fahren nach Level 4 und 5 möglich ist. Letztendlich soll TP4 die Frage beantworten, was und wie im Kontext des autonomen Fahrens der Stufe 4 und 5 getestet werden muss.

Zielsetzung von TP4 ist die Schaffung eines methodischen Ansatzes zur Ableitung von System- und Testanforderungen am Beispiel des Use Case Urbane Kreuzung. Dazu werden Methoden entwickelt (AP4.1), wie aus der funktionalen Systemarchitektur und dem notwendigen Sicherheitskonzept nicht-wettbewerbsdifferenzierende System- und Testanforderungen bestimmt werden können (= Reifestufen der Methodik). Die Methodenentwicklung erfolgt zunächst anhand des ersten Entwurfs der funktionalen Systemarchitektur und des lokalen Sicherheitsziels (aus TP3). Sie werden anschließend sukzessive verfeinert, um Wahrscheinlichkeiten von Kritikalitäten und Degradationen berücksichtigen zu können. Dabei werden die Erkenntnisse aus den FOTs sowie die kontinuierlichen Detaillierungen der funktionalen Systemarchitektur, der lokalen und globalen Sicherheitsziele und deren Gütekriterien berücksichtigt. Die Plausibilität und Anwendbarkeit der entwickelten Methoden wird exemplarisch für den Use Case Urbane Kreuzung in den Arbeitspaketen Systemanforderungen (AP 4.2) und Testanforderungen (AP 4.3) untersucht.

3.1.2.4.1 Goal – Question – Metric (GQM)

Einführung und aktueller Stand der Technik

Goal Question Metric [94] ist eine Methode, die entwickelt wurde, um Ziele von Organisationen und deren Projekten zu messen. Im Rahmen des Projekts VVM verwenden wir die ersten drei Schritte, um quantitative Antworten auf Fragen abzuleiten. Diese Fragen werden aus mehreren Inputs abgeleitet. Inputs, die Teil des Entwicklungsprozesses eines Systems sind, sowie soziale, regulatorische und andere Inputs für das System als ein mit der Welt interagierendes Produkt. Diese quantifizierbaren Antworten liefern Metriken, die eine Grundlage dafür bilden, wie das System entworfen und getestet werden muss. Eine Interaktion zwischen dem GQM-Modell, das einen Katalog dieser Metriken darstellt, und dem Requirements Engineering sowie probFMEA & CFT wurde auf der Halbzeitveranstaltung des VVM-Projekts vorgestellt. [95]

Entwicklung innerhalb VVM

Zu diesem Zeitpunkt haben wir die folgenden Inputs betrachtet, den GQM-Prozess verfolgt und somit Metriken für sie katalogisiert (siehe Abbildung 169).

- Aus der fähigkeitsbasierten Architektur abgeleitete Anforderungen
- Bekannte Messgrößen wie Time to Collision
- Fähigkeiten der Komponenten,
- Gespräche mit Experten, welche relevanten Fragen sich in Bezug auf den Einsatz von Lidar in der Automobilindustrie stellen.

Diese quantifizierbaren Antworten liefern Metriken, die eine Grundlage dafür bilden, wie das System entwickelt und getestet werden muss.

Erstellung und Pflege des Modells

Ein Ziel wird durch seinen Zweck, ein Problem, ein damit verbundenes Objekt oder einen Prozess und schließlich einen Gesichtspunkt definiert. Ein Beispiel hierfür wäre "Verbessere das Verständnis von GQM für den Leser dieses Kapitels".

Im Hinblick auf das vorgegebene Ziel können mehrere Fragen definiert werden, und anschließend können Metriken entwickelt werden, um diese Fragen zu beantworten. Einige oder alle dieser Metriken können dann zur Beantwortung von Fragen in Bezug auf ein Ziel innerhalb eines beliebigen verbrauchenden Prozesses im Entwicklungsprojekt verwendet werden.

Die Pflege des Modells folgt dann den iterativen Anforderungen des Gesamtprojekts.

Im VVM-Kontext erstellte Modelle

Es wurden 2 Modelle erstellt. Das eine ist ein allgemeines Modell, das für E4.1a erstellt wurde, sowie eine aktualisierte Version, die in E4.1d einfließt. Die aktualisierte Version enthält auch ein zweites Modell, das die GQM für ein LIDAR katalogisiert. Diese Modelle sind in MS Excel-Tabellen niedergeschrieben.

Verwendung im VVM

Auszüge aus beiden Modellen wurden in Prob FMEA & CFT Tool SafeTBox modelliert.

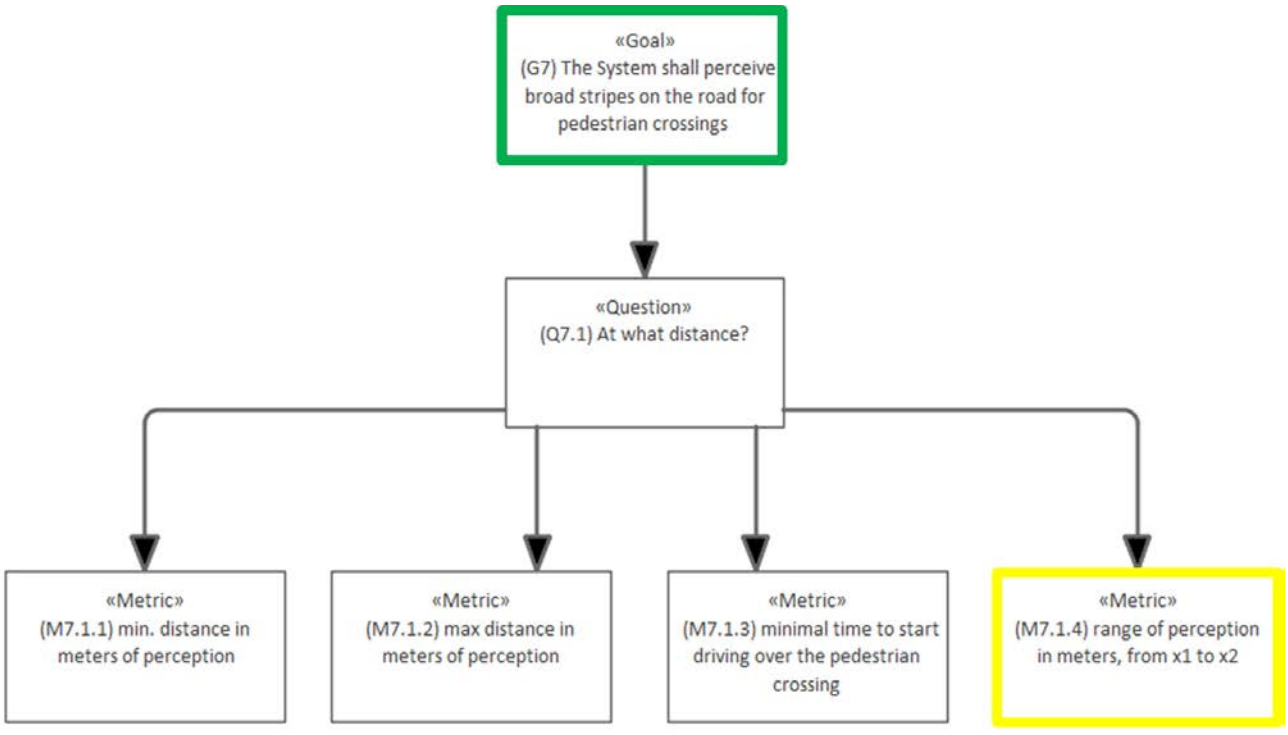


Abbildung 169: Modellauszug für GQM

Im Hinblick auf die Anforderungsentwicklung wurde das GQM-Modell auch als Input verwendet, um nicht-funktionale Anforderungen für gegebene funktionale Anforderungen abzuleiten. Wenn es für eine gegebene funktionale Anforderung keine passende Metrik gab, wurde das GQM-Modell rweitert, um eine Metrik zu entwickeln, die dann als Input für eine neue nicht-funktionale

Anforderung verwendet werden kann. Ein Auszug aus den Anforderungen mit Bezug zum GQM-Modell ist in Tabelle 5 zu sehen.

Tabelle 5: Anforderungen mit Bezug zum GQM-Modell

ID	Title	System Requirement	Req. Type	Refines
SR-3.1.2	crosswalk marking perception	The system shall **perceive** broad stripes on the road for *crosswalk markings*.	Functional	
SR-3.1.2a	crosswalk marking perception **range**	The system shall **perceive** crosswalk markings on the vehicle's traffic lane in a distance at least between x and *y* meters in the direction of driving.	Performance	**SR-3.1.2**

3.1.2.4.2 Sicherheitsanalyse von (Un-)Fähigkeiten und Schwachstellen mit Component Fault Trees und probFMEA

Methodischer Ansatz für Sicherheitsanalysen im Kontext von Anwendungsfällen mittels eines kombinierten Top-down- und Bottom-up-Analyseverfahrens

Der vorgestellte Ansatz kombiniert ein Top-down-Analyseverfahren auf Basis von Component Fault Trees (CFT) mit der Bottom-up-Technik probFMEA (Abbildung 170). Im Rahmen des VVM Projektes wurde dabei der CFT Ansatz, welcher in der klassischen Variante auf funktionale Sicherheit abzielt, um eine konzeptionelle Erweiterung zur Abdeckung von SOTIF Aspekten (Safety Of The Intended Functionality) erweitert. In dieser Kombination ermöglicht dies eine systematische Systemanalyse, die sowohl die klassische funktionale Sicherheit als auch Aspekte von SOTIF auf verschiedenen Abstraktionsebenen berücksichtigt und so den ganzen Entwicklungszyklus unterstützt.

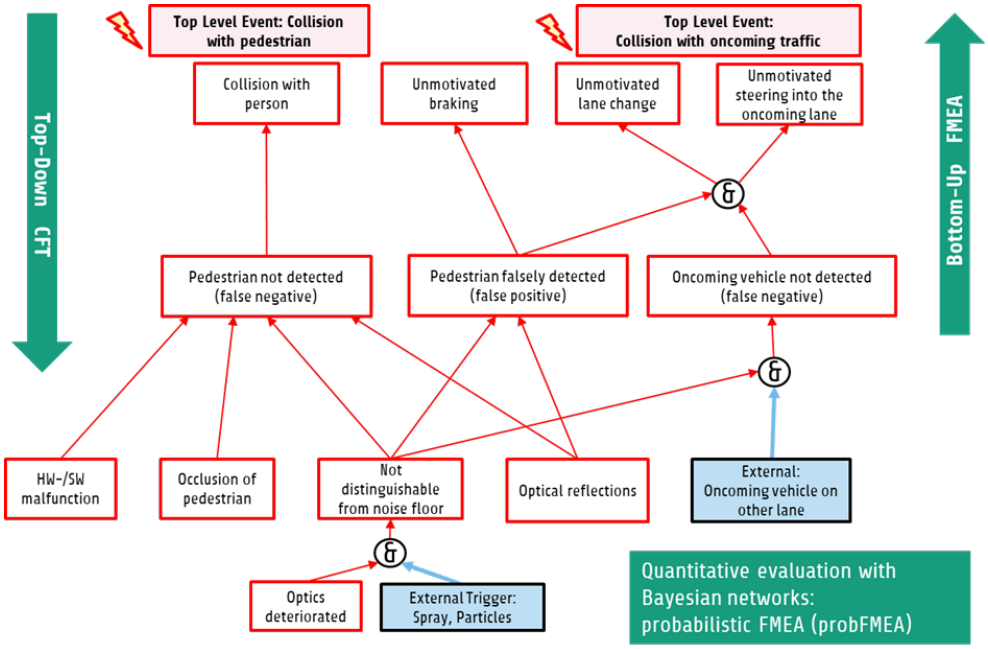


Abbildung 170: Sicherheitsanalyse mit Top-Down Component Fault Tree (CFT) und Bottom-Up probFMEA

Die erarbeiteten Erweiterungen sind jeweils:

CFT: Erweiterung der Fehlerbaumanalyse (FTA) um eine direkte Verbindung und Rückverfolgbarkeit zu den Elementen der Systemarchitektur.

probFMEA: Komponentenbasierte Erweiterung von FMEA um probabilistische Argumentationen zu Ursache-Wirkung-Beziehungen.

Abbildung 171 fasst die Eigenschaften und Leitfragen der beiden Methoden in Abhängigkeit von der Sicht und der Abstraktionsebene zusammen.

View	Layer	Analysis content	CFT (identification)	probFMEA (deduction)
Behavioural	Ego behaviour (in scenario)	Behavioural deviations and failures	Which capability deficits and deviations can lead to certain behavioral deviations?	Which undesired behavior and effects can possible capability deficits lead to in the specific scenario?
Capability-based taxonomy	Capabilities	Capability deficits	Which functional weaknesses and deviations can lead to specific capability deficits?	Which capability deficits do functional failures and weaknesses lead to?
Technical	System structure	Weaknesses and deviations from intended function	Which failure in parts and data processing errors could occur to cause the assumed system failure?	What functional deviations can possible component and software failures lead to?
	Component / item	Defects and failures of individual elements, components, software		

Abbildung 171: Ergebnisse der CFT und probFMEA Analyse hängen von der Sicht und Abstraktionsebene ab.

Die neue Methode hat folgende Eigenschaften bzw. bietet folgende Möglichkeiten:

- Anwendbar auf verschiedenen Abstraktionsebenen: auf den Systemfähigkeiten basierende Taxonomie, funktionale und technische Architektur.
- Modellierung der Sicherheitsauswirkungen von System(un)fähigkeiten und –schwachstellen.
- Verifizierung von Sicherheitsmaßnahmen und Verbesserung der Risikominderung.
- Ableitung und Verfeinerung von Sicherheitsanforderungen und Identifizierung neuer Top-Level-Ereignisse durch einen Bottom-up-Ansatz.
- Identifizierung neuer Testanforderungen.
- Verifizierung der Übereinstimmung mit dem Zielverhalten und den Sicherheitsanforderungen.
- Bereitstellung qualitativer und quantitativer Nachweise für die Sicherheitsargumentation.

Die Schritte der Methodik

- Schritt 1: Die auf den Systemfähigkeiten basierende Taxonomie als Voraussetzung liefert Systemfähigkeiten und analysiert die aktiven Fähigkeiten für den Anwendungsfall.
- Schritt 2: Die Analyse beginnt mit einem für einen bestimmten Anwendungsfall formulierten Top-Level-Element (TLE) (z. B. Verstoß gegen eine Sicherheitsanforderung). Durch Verwendung von Schlüsselwörtern werden systematisch die Ursachen für den Verstoß identifiziert. Zur Modellierung der Fehlerfortpflanzung werden Abhängigkeiten aus Schritt 1 als Rankhilfe verwendet.

- Schritt 3: Der Einfluss der verwendeten Technologien auf den konkreten Anwendungsfall wird modelliert. Dazu werden sensorspezifische Kataloge zur Auswahl von SOTIF-Aspekten wie Auslösebedingungen und Schwachstellen als Basisereignisse in CFTs herangezogen. Dabei werden aus der Goal-Question-Metric-Methode abgeleitete Qualitätskriterien und Metriken angewandt.
- Schritt 4: Analyse der CFTs im Hinblick auf die kritische Kombination von Auslösebedingungen und Schwachstellen, sowie Einzelpunktfehlern, die zu einer Verletzung des gewählten TLE (z.B. einer Sicherheitsanforderung) aus Schritt 2 führen. CFTs werden für eine erweiterte quantitative Analyse automatisch in Bayes'sche Netze (BN) übersetzt.

Die qualitativen und quantitativen Analyseergebnisse von probFMEA, CFT und BN dienen als Nachweise für die Sicherheitsargumentation. Die architekturbasierte Fehlermodellierung mit CFTs, unter Einbeziehung von Unzulänglichkeiten, ermöglicht eine Komponentensicht auf Fehler. Mithilfe von probFMEA und den darunterliegenden BNs können in einem Modell verschiedene Szenarien und Parameter variiert werden. CFTs und probFMEA ermöglichen somit die Sicherheitsanalyse komplexer Systeme [95].

safeTbox: Modellbasiertes Safety Engineering

Die zunehmende Komplexität moderner sicherheitskritischer eingebetteter Systeme erfordert eine Skalierung und neue Entwicklungs- und Dokumentationsansätze. Das Fraunhofer IESE stellt sich dieser Herausforderung durch die Erforschung und Entwicklung integrierter modellbasierter Safety-Engineering-Ansätze, mit einem starken Fokus auf Architekturintegration, Verfolgbarkeit, Wiederverwendbarkeit und Wartbarkeit sicherheitsrelevanter Artefakte. Die Hauptfunktionen von safeTbox sind Architekturentwurf, Gefahren- und Risikoanalyse, Sicherheitsanalysen mittels CFT, und Sicherheitsargumentation mittels der Goal Structuring Notation. safeTbox ist ein Plugin für Enterprise Architect und ermöglicht die direkte Integration und Verlinkung der Fehlermodelle mit den Komponenten der Systemarchitektur (siehe Abbildung 172).

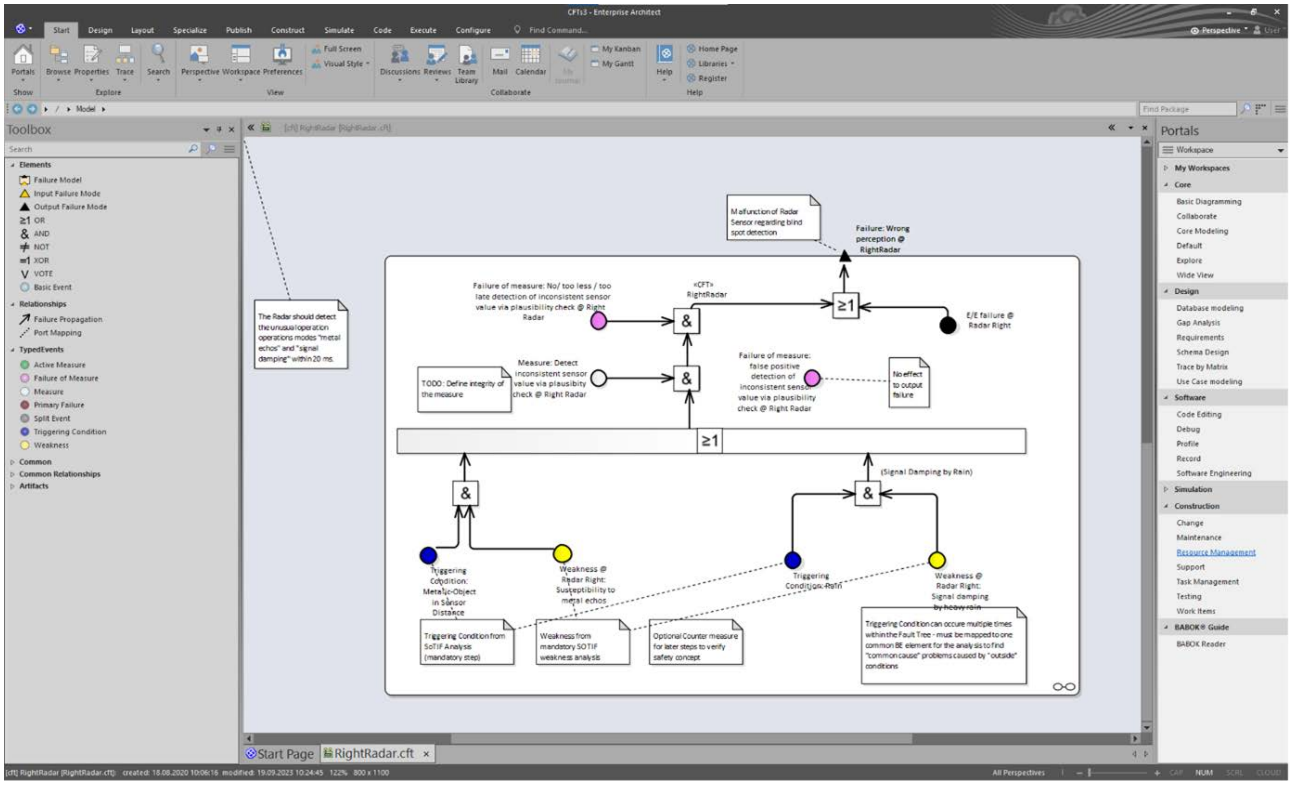


Abbildung 172: Fehlerpropagierung mit SOTIF Aspekten modelliert in safeTbox

Erweiterung von safeTbox für SOTIF-Aspekte

Im Rahmen des VVM Projektes wurde safeTBox und insbesondere die Sicherheitsanalyse mittels CFTs um eine Unterstützung für SOTIF Aspekten erweitert. Hierbei wurden spezifische Typen von Basic Events für die Berücksichtigung von SOTIF Aspekten definiert. Dies erlaubt eine Abgrenzung von den Aspekten, welche die klassische funktionale Sicherheit betreffen, ermöglicht aber gleichzeitig die Modellierung beider Aspekte innerhalb eines Fehlermodells. Die folgende Liste zeigt die neu eingeführten Typen zur Abbildung der SOTIF-Aspekte:

- Schwachstelle: Unzulänglichkeit oder Untauglichkeit eines Sensors oder einer Sensorverarbeitung (wie z.B. einer Anfälligkeit für bestimmte Wetterphänomene).
- Auslösebedingung: Möglicher Grund für die Auslösung einer Schwachstelle (wie z.B. dem aktuellen Auftreten einer Umweltbedingung oder eines Wetterphänomens).
- Ausgelöste Schwachstelle: Zwischenereignis, dass ein Systemversagen darstellt.
- Versagen einer Maßnahme: Ereignis, das eine nicht ordnungsgemäß behobene ausgelöste Schwachstelle darstellt.

Typisierte Ereignisse ermöglichen automatische Prüfungen auf Konsistenz in der Modellierung. Außerdem ist es aufgrund der Wiederverwendung von Komponenten möglich, Wissen über Schwachstellen und Auslösebedingungen von Sensoren und Verarbeitungsprozessen wiederzuverwenden. Darüber hinaus liefern Typen zusätzliche Informationen zur sinnvollen Interpretation der Ergebnisse von Sicherheitsanalysen.

Ablauf der Modellbasierten Sicherheitsanalyse mit safeTbox (siehe Abbildung 173):

Schritt 1: Modellierung hierarchischer Fähigkeiten

Die Abhängigkeiten zwischen den Fähigkeiten werden als Ports modelliert, wobei diese Struktur als Input für das auf die Architektur abgestimmte Fehlerfortpflanzungsmodell dient.

Schritt 2: Modellierung der Fehlerpropagierung auf Grundlage der Abhängigkeiten

Die Analyse beginnt mit einem Top-Level-Element. Die Ursachen für die Fehler werden anhand der modellierten Abhängigkeiten bis zum atomaren Element der analysierten Abstraktionsebene zurückverfolgt. Auf der Ebene der Abhängigkeiten und Ereignisse werden Schlüsselwörter verwendet, um die systematische Identifizierung der Fehlerursachen zu ermöglichen.

Schritt 3: Modellierung von Fehlerursachen unter Berücksichtigung von Qualitätsmaßnahmen und mit Bezug auf SOTIF

Der Einfluss der eingesetzten Technologien auf den spezifischen Anwendungsfall wird ebenso modelliert wie Verstöße gegen die erforderlichen Qualitätsmessungen.

Schritt 4: Qualitative Analysis mit Minimal Cut Sets

Es wird eine Sicherheitsanalyse durchgeführt, um die Auslösebedingungen für das Testen und ausgelöste Schwachstellen ohne/mit unzureichenden Gegenmaßnahmen zu identifizieren.

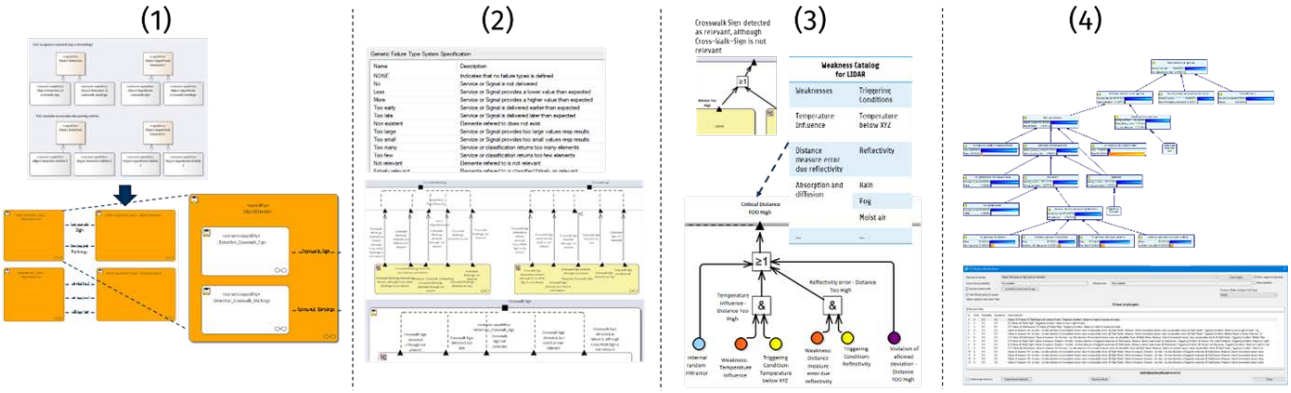


Abbildung 173: Schritt 1 bis 4 der Modellierung von Fähigkeiten: (1), Fehlerpropagierung (2), Fehlerursachen mit Qualitätsmaßnahmen (3) und qualitative Minimal Cut Sets Analyse (4)

3.1.2.4.3 Anforderungen für die Testplanung

Systemanforderungen

Die Systemanforderungen basieren auf den Bedürfnissen der Stakeholder und den Verhaltensanforderungen.

Stakeholder Needs werden aus verschiedenen Quellen gesammelt, wie z.B. funktionalen Anwendungsfällen, einer Objektdefinition oder Kundenfunktionen.

Verhaltensanforderungen spezifizieren die Anforderungen der Stakeholder an das Verhalten in einem szenariospezifischen Kontext.

Viele Anforderungen an das automatisierte Fahren sind durch Sicherheitsaspekte motiviert. Daher werden Sicherheitsaspekte durch zwei weitere Quellen abgedeckt:

Safety Goals sind Top-Level-Sicherheitsanforderungen, die sich aus der Gefahrenanalyse und Risikobewertung auf Fahrzeugebene ergeben. [94]

Behavioral Safety Requirements spezifizieren lösungsunabhängiges sicherheitsrelevantes Verhalten oder lösungsunabhängige Sicherheitsmaßnahmen einschließlich ihrer sicherheitsrelevanten Eigenschaften.

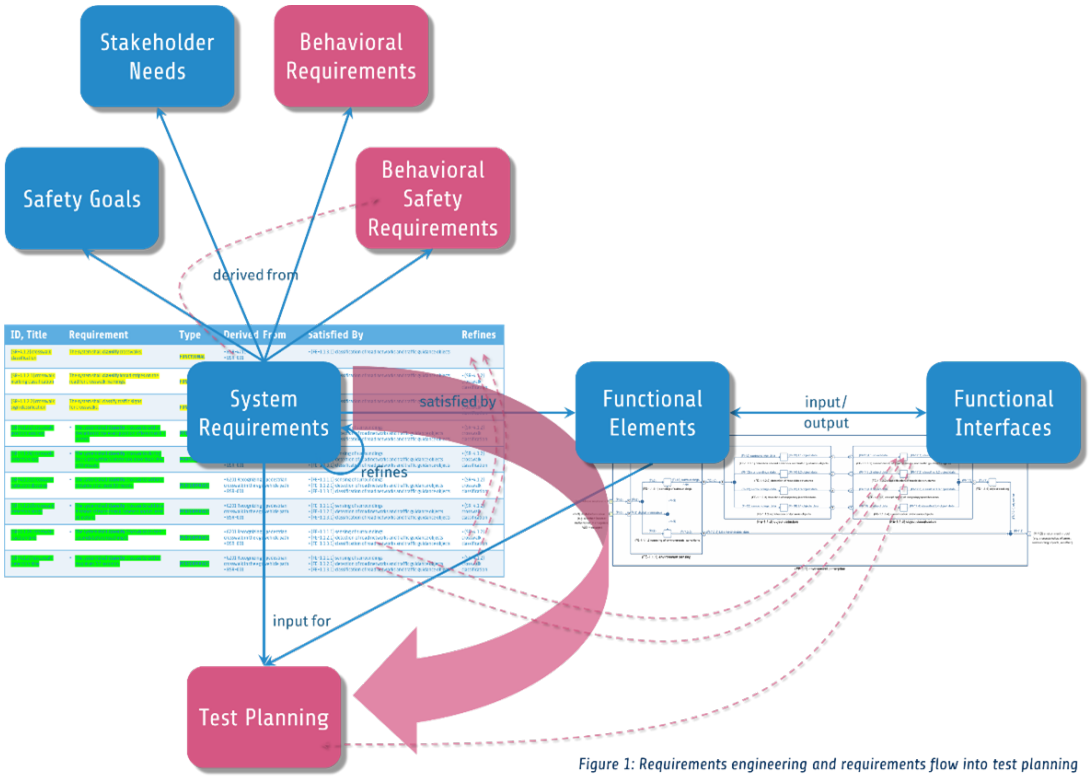


Abbildung 174: Schematischer Ablauf des Ableitens der Testplanung aus den Systemanforderungen

Übergabe an die Testplanung (Abbildung 174)

Die Funktionselemente der Funktionalen Architektur werden als Testobjekte an die Testplanung übergeben. Funktionale Elemente bündeln ihre zugehörigen Systemanforderungen. Die enthaltenen Leistungsanforderungen sind Ziele bei der Festlegung von Pass/Fail-Kriterien für das Testen.

Die Anwendung der Goal/Question/Metric (GQM) Methode [96] auf ausgewählte Funktionale Anforderungen führt zu Qualitätskriterien. Diese werden als Leistungsanforderungen formuliert und verfeinern die funktionalen Anforderungen.

Funktionale Anforderungen sind Aussagen, die festlegen, welche Ergebnisse ein Produkt oder ein Prozess erzeugen soll. [94]

Leistungsanforderungen sind messbare Kriterien, die angeben, [...] wie gut die funktionalen Anforderungen erfüllt werden sollen. [94]

Funktionale Architektur

Eine funktionale Architektur erfüllt die Systemanforderungen, indem sie ausreichende Funktionalität definiert. Während der Ausarbeitung der funktionalen Architektur werden parallel dazu die Systemanforderungen verfeinert.

Eine funktionale Architektur ist eine hierarchische Anordnung von Funktionen, ihren internen und externen funktionalen Schnittstellen und externen physischen Schnittstellen, ihren jeweiligen Funktions- und Leistungsanforderungen und ihren Entwurfseinschränkungen. [94]

3.1.2.4.4 Testplanung

Einführung

In der Testplanung wird die Menge aller funktionalen Testfälle definiert. Ein einzelner oder eine Gruppe gleichartiger funktionaler Testfälle wird durch eine funktionale Testspezifikation beschrieben, die alle für diesen Testfall oder diese Testfallgruppe relevanten funktionalen Testanforderungen bündelt. Die funktionalen Testspezifikationen stellen somit den funktionalen Testraum als zentrales Ergebnis der Testplanung dar. Im Wesentlichen geht es darum, die entsprechenden funktionalen Testobjekte und Szenarien auszuwählen und sie mit den gewünschten Testzielen einander zuzuordnen, d.h. mit Testfällen zu verbinden.

Strukturierung der Testplanung

Die Auswahl der funktionalen Testobjekte basiert auf dem funktionalen Entwurf in Form einer funktionalen Architektur und den damit verbundenen funktionalen Anforderungen einschließlich ihrer Güten (siehe Abbildung 175). Die Testszenarien können aus der Gesamtmenge aller evaluierten Szenarien ausgewählt werden. Diese, im Kontext der VVM auch als "Logical Scenario Instances" bezeichnet, repräsentieren die ODD vollständig und werden in ihrer Eintrittswahrscheinlichkeit bewertet.

Die Motivation für den Testfall wird in den Testzielen ausgedrückt. Zunächst wird hier grundsätzlich zwischen Verifikation und Validierung unterschieden. Während bei der Verifikation geprüft wird, ob das Produkt die Anforderungen erfüllt, geht es bei der Validierung um die Frage, inwieweit das Produkt seinen Verwendungszweck erfüllt. In beiden Fällen wird konkret beschrieben, was gemessen werden soll, um den für die Argumentation notwendigen Nachweis zu erbringen.

In der realen Welt sind die möglichen Kombinationen von Testobjekten, Umgebungen und Zielen endlos. Um sich auf eine in der Praxis umsetzbare Menge von Testfällen zu beschränken, wird eine Gewichtung nach den sicherheitssensitiven Bereichen vorgenommen. Dazu wird ein Modell benötigt, das die einzelnen Funktionen und Szenarien aus der Dekomposition von funktionalem Design und ODD hinsichtlich ihrer Bedeutung für die Sicherheit bewertet und quantitativ beschreibt.

Ein Sonderfall in diesem zunächst top-down strukturierten Ansatz sind die Bedenken. Dabei handelt es sich um Hinweise subjektiver (z. B. Bewertungen) oder objektiver (z. B. Messergebnisse) Natur, die hinsichtlich des Testumfangs besonders berücksichtigt werden müssen. Bedenken können in verschiedene Klassen eingeteilt werden. Funktionale Belange beziehen sich beispielsweise auf die funktionale Gestaltung, während Szenario-Belange sich auf Szenarien beziehen, die berücksichtigt werden müssen. Je nach Klassifizierung werden solche Bedenken an der entsprechenden Stelle aufgenommen, um ihre Sicherheitsrelevanz im Kontext des funktionalen Designs oder der logischen Szenarieninstanzen zu gewichten und im Rahmen der Tests zu berücksichtigen.

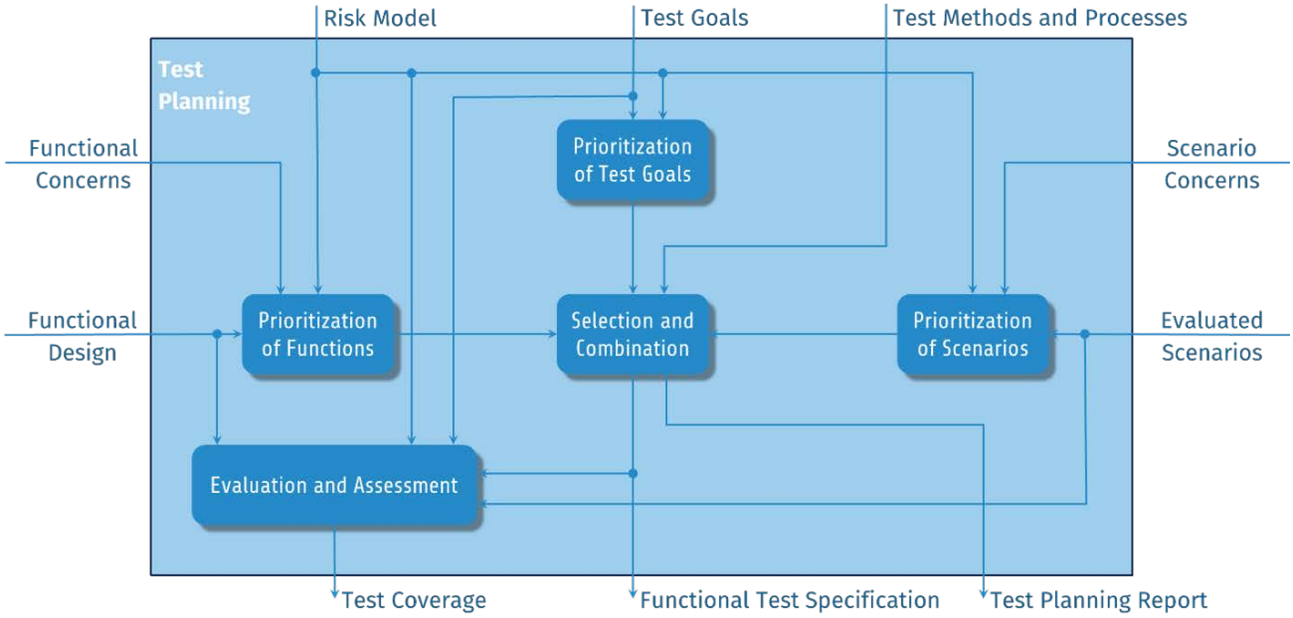


Abbildung 175: Darstellung der Testplanung inkl. der In- und Outputs

Funktionale Testspezifikation

Wie bereits beschrieben, ist die funktionale Testspezifikation der zentrale Output der Testplanung, der an die Testorchestrierung übergeben wird. Dort wird sie dann mit Hilfe des technischen Entwurfs in die technische Testspezifikation überführt. Nur die technische Testspezifikation ist tatsächlich ausführbar.

Verifizierung

Die Verifikation dient dem Nachweis, dass das Produkt die vereinbarten Anforderungen erfüllt. Für die funktionale Testspezifikation bedeutet dies, dass beschrieben werden muss, in welchen Testszenarien welcher funktionale Testgegenstand in Bezug auf welche Zielgrößen untersucht werden muss. Abbildung 176 zeigt das konkrete Beispiel einer in VVM entworfenen funktionalen Prüfvorschrift für die Verifikation.

Nach dem Identifikator und der eindeutigen Bezeichnung der funktionalen Testspezifikation werden über die nächsten Attribute die Testszenarien beschrieben. Dabei sind zwei Informationen wesentlich: das logische Szenario und die Variationsregel. Zunächst wird das zugrundeliegende funktionale Szenario beschrieben sowie die deklarierten Parameter einschließlich der Räume möglicher Parameterwerte und deren Grenzen. Danach folgt die Information über die Variation des Szenarios. In diesem einfachen Beispiel sind mit einer Ausnahme alle Parameterwerte fest vorgegeben und nur die Sichtbarkeit wird variiert. Die Schrittweite durch diesen Parameterraum wird mit einem konstanten Wert angegeben. Es ist auch denkbar, dass an dieser Stelle Variationsalgorithmen festgelegt werden. Auf dieser Basis ist es anschließend möglich, konkrete Szenarien bei der Testdurchführung zu generieren.

Bei der Beschreibung des funktionalen Prüfobjekts wird auf die funktionale Architektur und die Systemanforderungen Bezug genommen. Konkret wird auf das funktionale Element und dessen Beschreibung in der Architektur und Spezifikation verwiesen. Im vorliegenden Beispiel ist das Funktionselement (FE) "Klassifizierung von Straßennetzen und Verkehrsleitobjekten".

Die zugrundeliegenden Systemanforderungen spezifizieren das Funktionselement und geben Auskunft über die zu prüfenden Güten. Für Informationen darüber, wie diese Güten zustande gekommen sind, wird hier auf die GQM verwiesen.

Neben der nachzuweisenden Güte ist für die Prüfplanung wesentlich, mit welchem Vertrauen der Nachweis der Güten geführt werden soll. Diese Vertrauensanforderung kommt aus der Sicherheitsmodellierung und steht der Testplanung als Input zur Verfügung. Sicherheitsziele werden im Rahmen der Verifikation nicht explizit erwähnt, weil hier die Güten wesentlich sind, die über die Systemanforderungen auf die Sicherheitsziele zurückgeführt werden können.

Die Prüfziele werden aus den zu verifizierenden Qualitäten und der Vertrauensanforderung gebildet. Ein Beispiel ist in Attribut 6 in Abbildung 176 dargestellt. Implizit werden an dieser Stelle Testabbruchkriterien für den Fall angegeben, dass ein Testziel aufgrund unzureichender Performance nicht erreicht werden kann.

Die funktionale Testspezifikation endet mit Attribut 7, das die Möglichkeit bietet, Angaben zu Testklassen und Methoden zu machen.

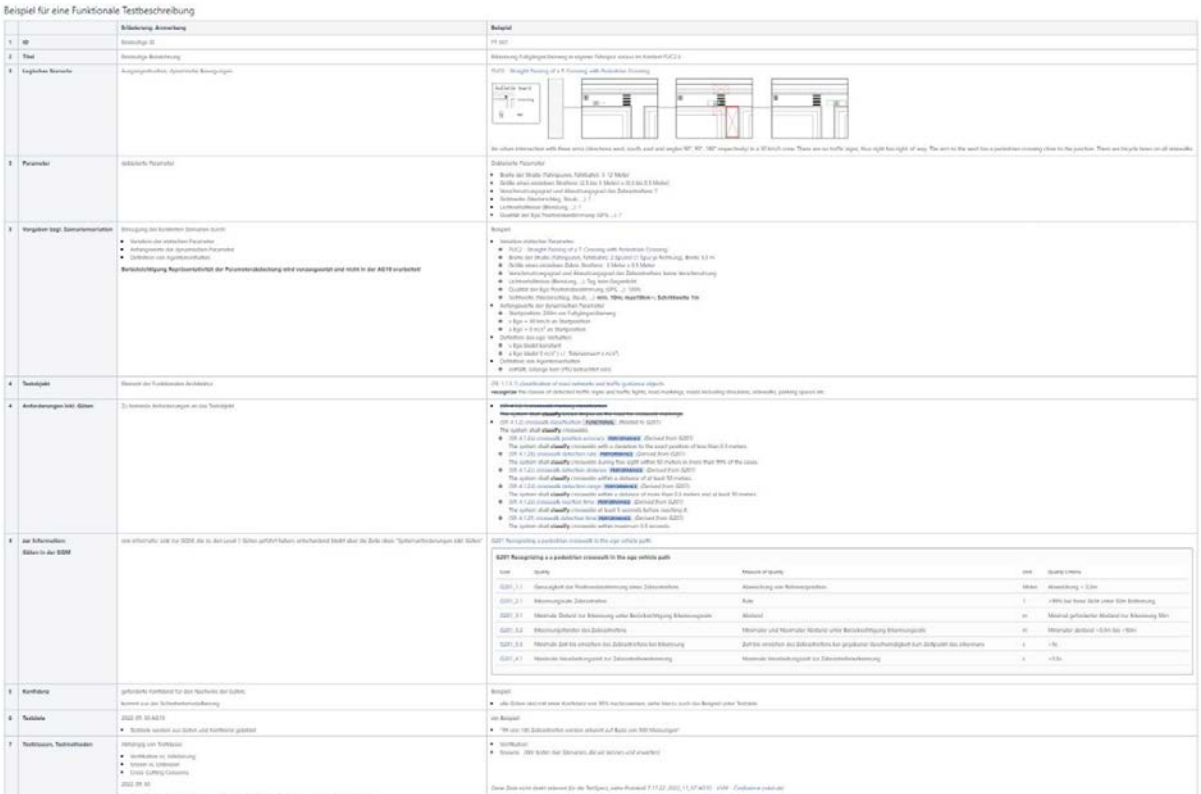


Abbildung 176: Beispielhafte Funktionale Testspezifikation für die Verifikation

Validierung

Die Validierung verfolgt das Ziel, den Nachweis zu erbringen, inwieweit das Produkt seinen vorgesehenen Zweck erfüllt. In diesem Zusammenhang steht auch der Nachweis der Sicherheit im Mittelpunkt der VVM. Dazu muss die funktionale Testspezifikation konkret beschreiben, was gemessen werden muss, um die für die Sicherheitsargumentation erforderlichen Nachweise zu erbringen.

Die funktionale Testspezifikation für die Validierung folgt grundsätzlich der gleichen Struktur wie die für die Verifikation. Auch die Validierung muss über das funktionale Testobjekt, die funktionalen Zielvariablen und die Umgebung, d.h. die Testszenarien, gesteuert werden. Allerdings gibt es Unterschiede im Inhalt. Abbildung 4.9 zeigt das konkrete Beispiel einer in VVM entworfenen funktionalen Testspezifikation für die Validierung.

Während die Verifikation den bekannten Raum über relevante, detailliert spezifizierbare Testszenarien abdeckt, muss die Validierung in den unbekannten Raum vordringen und kritische unbekannte Szenarien finden. Die funktionale Testspezifikation erfordert daher eine zufällige und vielseitige Durchquerung des ODD.

Der funktionale Prüfgegenstand bewegt sich im Allgemeinen auf hohen Systemebenen, d. h., wie z. B. in Abbildung 177, auf der Ebene der ADS-Funktion.

Bezüglich der funktionalen Zielgrößen muss im Rahmen der Validierung von den Validierungskriterien gesprochen werden. Im vorliegenden Beispiel wird davon ausgegangen, dass die kritische Bremsung im Rahmen der Kollisionsvermeidung über einen Quotienten aus notwendiger Verzögerung und maximal möglicher Verzögerung identifiziert werden kann. Die Funktionsprüfungsspezifikation muss Auskunft darüber geben, welche Werte zu messen sind, welche Werte aus Messwerten zu berechnen sind, welche Schwellenwerte gelten und welche statistische Auswertung zu bilden ist.

Beispiel für eine Funktionale Testbeschreibung

		Erläuterung, Anmerkung	Beispiel
1	ID	Eindeutige ID	FT-101
2	Titel	Eindeutige Bezeichnung	Einhalten unkritischer lateraler Abstände im Kontext FUC2.3
3	Umgebung	Ziel im Rahmen der Validierung ist es, die ODD zufällig und vielseitig zu durchfahren, um kritische Unknowns finden zu können.	
4	Testobjekt	ADS-Funktion (Damit ist das gesamte funktionale System gemeint.)	TP4 AG9 AD Funktionale Systemarchitektur
4	Validierungskriterien (=tragenommen sind Validierungs-Maße gemeint)	Es muss nachgewiesen werden, welche Sicherheitsreserve im Falle einer Kollisionsvermeidung besteht. Als KPI müssen Kritikalitätsmaße herangezogen werden. Für dieses Beispiel ziehen wir folgenden KPI heran: • benötigte Verzögerung als Funktion von Geschwindigkeit und Abstand im Verhältnis zur max. möglichen Verzögerung • max. mögliche Verzögerung hängt vom Reibwert ab → wenn der Reibwert nicht mit gemessen werden kann, muss hier eine Vorgabe gemacht werden	zu messen: • Geschwindigkeit des Fahrzeugs in X-Richtung • Abstand zum Fußgänger in X-Richtung • Bezugsgröße: gefahrene Strecke, gefahrene Zeit, durchfahrene Szenarien zu berechnen: • benötigte Verzögerung, um Kollision zu vermeiden • benötigte Verzögerung / max. möglicher Verzögerung
4	Gütekriterien	1. Gütekriterium (z.B. Schwellwert für die Kritikalität). 2. Statistische Auswertung (inkl. Konfidenzbestimmung): Überschreitung des Gütekriteriums (z.B. Schwellwert) je km, h, Anzahl Szenarien.	1. Schwellwert liegt bei 0,5 (50% der max. möglichen Verzögerung) 2. tbd
4	Messdaten/Messgrößen	2023_07_17: Zeile neu eingefügt Für die Auswertung benötigte Informationen, zB: • um die Ursachen analysieren zu können, warum das Gütekriterium eines Validation Criteria verletzt wurde	Bzgl: • Kameraraten/s/Bildaufzeichnungen • Daten aus dem Ego-Fahrzeug zu: o Bewegung o Umfeld o etc.

Abbildung 177: Beispielhafte Funktionale Testspezifikation für die Validierung

Zusammenfassung und Ausblick

Wie oben erläutert, wird die funktionale Testspezifikation auf der Grundlage des V&V-Konzepts entwickelt und bildet einen wesentlichen Input für die technische Testorchestrierung. Sie basiert auf der funktionalen Architektur und gibt Auskunft darüber, welche Qualitätskriterien mittels welcher Metriken (die funktionalen Zielmetriken) für jeden Funktionsblock (die funktionalen Testobjekte) nachgewiesen werden müssen. Auch die entsprechenden Testszenarien werden dort genannt. Die funktionale Testspezifikation ist nicht ausführbar, bietet aber einen stabilen Rahmen für die Planung der technischen Testorchestrierung. Erst mit dem technischen Entwurf können dann Qualitätskriterien und relevante Metriken auf die Subsysteme und Komponenten

heruntergebrochen werden. Zusammen mit Variationsregeln, die zu konkreten Szenarien führen, kann die technische Testspezifikation dann ausgeführt werden. Die Entscheidung über die konkrete Verteilung der Testfälle auf die Testinstanzen wird dann maßgeblich von den Fähigkeiten und der Validität der Testinstanzen bestimmt. Abbildung 4.10 stellt den Zusammenhang zwischen Testplanung und Testorchestrierung dar und zeigt die relevanten Inputs.

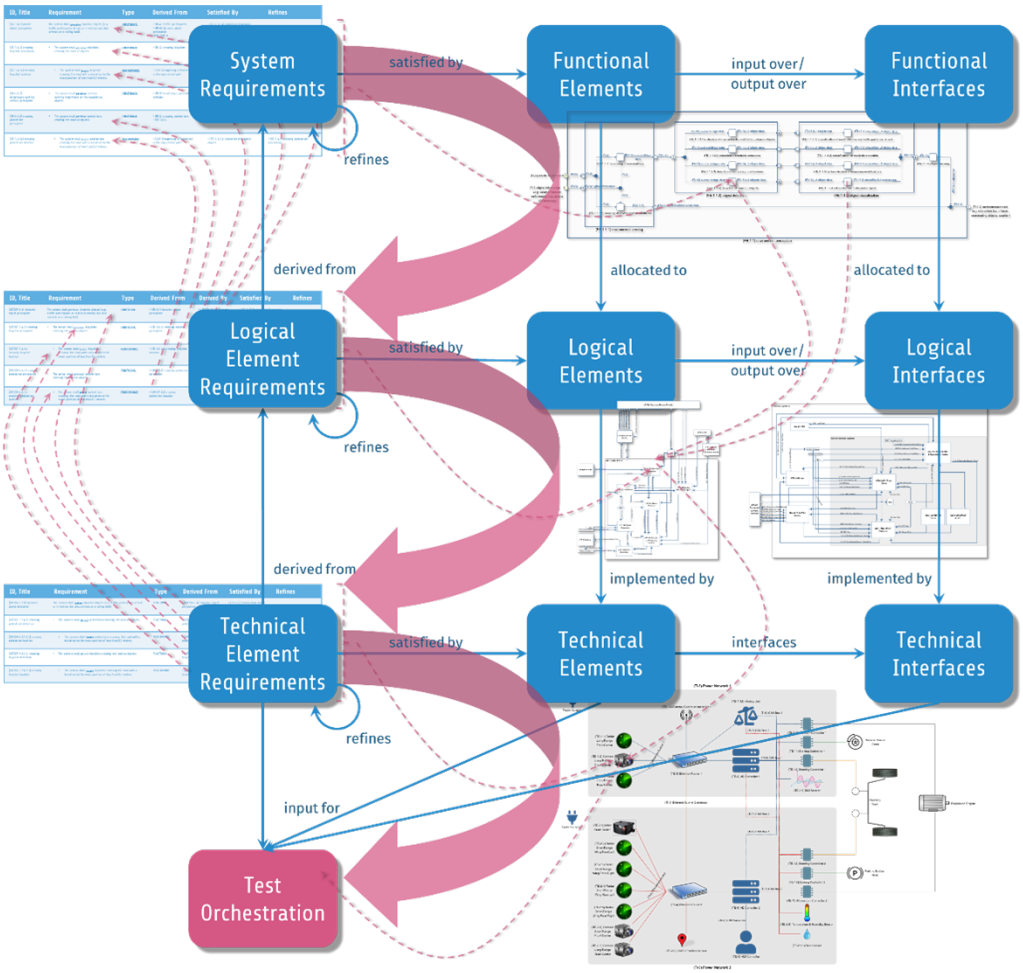


Abbildung 178: Inputs für die Testorchestrierung (siehe Kapitel 3.1.2.7)

3.1.2.5 TP5 Simulationssteuerung

Das TP5 untergliedert sich in zwei Arbeitspakete. Dem AP5.1 „Anforderungen an die Simulationstechnologie“ und dem AP5.2 „Verfügbarmachung und Instanziieren einer Simulationsumgebung“.

3.1.2.5.1 AP5.1 Anforderungen an die Simulationstechnologie

Im Rahmen von AP5.1 wurden die Anforderungen an die Simulationstechnologie diskutiert. Zu Beginn des VVMethoden-Projekts war es daher notwendig, dass TP5 die anfänglichen Anforderungen für die Hauptanwendungsgebiete der Simulation in VVMethoden - die Kritikalitätsanalyse und die Absicherung - ermittelte, formulierte und mit den vorhandenen Werkzeuglösungen abglich. Diese Anforderungen umfassten verschiedene Aspekte und wurden von den Projektpartnern während der relevanten Konkretisierungsphasen erarbeitet.

In Zusammenfassung beabsichtigt TP2, die Simulation zur Identifizierung der kausalen Zusammenhänge von Kritikalitätsphänomenen zu nutzen. Dabei werden zwei Anwendungsfälle

unterschieden: die Verfeinerung von Kritikalitätsphänomenen und die statistische Plausibilisierung von kausalen Zusammenhängen in der Kritikalitätsanalyse. Für diese Anwendungsfälle ergeben sich verschiedene Anforderungen an die Simulation. Um diese Anforderungen gezielt zu erfassen, hat der TÜV SÜD einen Fragenkatalog erstellt, der vom TP2 ausgefüllt wurde. Zusammenfassend ergeben sich folgende Anforderungen an die Simulation:

- Die Simulation muss in der Lage sein, kritische Verkehrsflüsse in weniger kritische oder stärker kritische Szenarien zu kategorisieren, um potenzielle kritische Szenarien zu bestimmen.
- TP2 möchte die Simulation für eine Effektivitätsanalyse nutzen, indem sie Ursachen zu einem kritischen Phänomen verschärft oder abmildert. Durch eine Vielzahl von Simulationsdurchläufen soll die Entstehung eines kritischen Szenarios identifiziert und die Robustheit gegenüber kritischen Phänomenen durch die Variation kritischer Parameter festgestellt werden.
- Die Simulation soll für die Identifizierung von Kritikalitätsphänomenen genutzt werden, die keine Auswirkungen auf die Kritikalität haben. Zudem soll es möglich sein, diese Phänomene in der Simulation zu analysieren.
- Die Interpretation der gewünschten Szenarien sowie die Simulation von abstrakten Szenarien mit Parametervariation stellen eine Herausforderung dar, da diese nicht ohne Weiteres simuliert werden können. Eine Simulation erfordert konkrete Szenarien.
- Die Evaluierung von Kritikalitätsmetriken sowie der Export der Simulationsergebnisse sind ebenfalls wichtige Anforderungen an die Simulation.

Des Weiteren hat das TP5 bei der Erstellung von exemplarischen Anforderungen an die Lidar-Simulation mitgewirkt. Die erstellten Anforderungen umfassten funktionale Testanforderungen, abgeleitete Anforderungen an die Gesamtsimulation, allgemeine Anforderungen an die Simulation des Sensormodells sowie Akzeptanztests für die Simulationsumgebung.

Das TP5 hat bei der Erstellung einer Wirkkette für das Lidar-Modell aus SetLevel beigetragen. In der Wirkkette wurden die physikalischen und technischen Zusammenhänge bei der Detektion von Lidar-Sensoren untersucht, wobei sowohl externe Bedingungen als auch Sensoreigenschaften eine Rolle spielten. Eine Relevanzanalyse der Wirkketten wurde durchgeführt, wobei die Auftrittswahrscheinlichkeit bestimmter Phänomene bestimmt wurde und anschließend die Auswirkungen auf die Funktionalität des gesamten Systems evaluiert wurden. Die resultierenden Werte wurden zu den finalen Relevanzen der Wirkketten aufsummiert. Basierend auf dieser Analyse wurden erste Anforderungen erstellt, die als Grundlage für exemplarische Tests in TP7 dienen können.

Zusätzlich wurde in enger Abstimmung von Valeo mit dSPACE und der TU Darmstadt die Simulationsumgebung Automotive Simulation Models (ASM) von dSPACE aufgesetzt und Punktwolken im PCD-Format erzeugt. Technische Anforderungen, wie die benötigte Positionsgenauigkeit, wurden in der Arbeitsgruppe Simulationsvalidierung erarbeitet.

Die Validierung der erzeugten Punktwolken erfordert ein realistisches Modell zur Reflektivität von Laserstrahlung an diversen Oberflächen, wobei die BRDF-Funktion in der dSPACE-

Simulationsumgebung genutzt wurde. In Zusammenarbeit mit dSPACE wurde Asphalt als erstes zu untersuchendes Material ausgewählt.

Zusätzlich wurde die Testumgebung des Valeo-Standorts in Kronach in der 3D-Grafiksuite Blender nachgebildet, um eine maximale Austauschbarkeit zwischen den verschiedenen Plattformen zur Sensorsimulation zu gewährleisten. Dies ermöglicht eine verbesserte Durchgängigkeit der Sicherheitsargumentation, wobei Valeo seine methodischen und technischen Aspekte zum Thema Lidar einbrachte.

Datengesteuerte Aggregation und Generierung von Szenarien zum Testen automatisierter Fahrfunktionen

Eine zentrale Forschungsfrage ist die Identifikation von sinnvollen und relevanten Verkehrsszenarien für ein Closed-Loop-Testverfahren. Abbildung 179 zeigt einen Überblick über die datenbasierte Generierung von selektiven Szenarien für das Testen hochautomatisierter Fahrzeuge und die im folgenden diskutierten Themen. Diese Pipeline umfasst eine Simulation von reaktiven Verkehrsszenarien, die mit Hilfe eines unüberwachten maschinellen Lernverfahrens gruppiert und in den Testraum eingeordnet werden.

Die Verkehrsszenen aus realen Aufnahmen werden in einen Graphen transformiert (siehe Abbildung 180), um die maschinelle Lesbarkeit und die Abstraktion der verschiedenen Straßenabschnitte zu verbessern [97]. Anschließend werden die Szenen zu funktionalen Clustern gruppiert und relevante Szenarien extrahiert. Um diese Szenen zu bevölkern, werden durch Nachahmungslernen trainierte KI-Modelle für alle anderen Verkehrsteilnehmer initialisiert. Dies ermöglicht ein reaktives Verhalten der Teilnehmer und erleichtert geschlossene Testverfahren für SUTs.

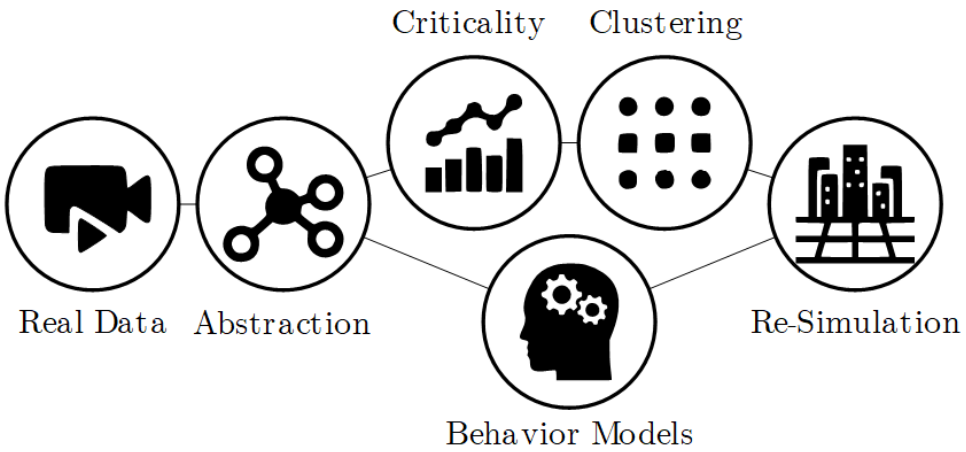


Abbildung 179: Szenariengenerierungspipeline und wichtige Beiträge (© FZI)

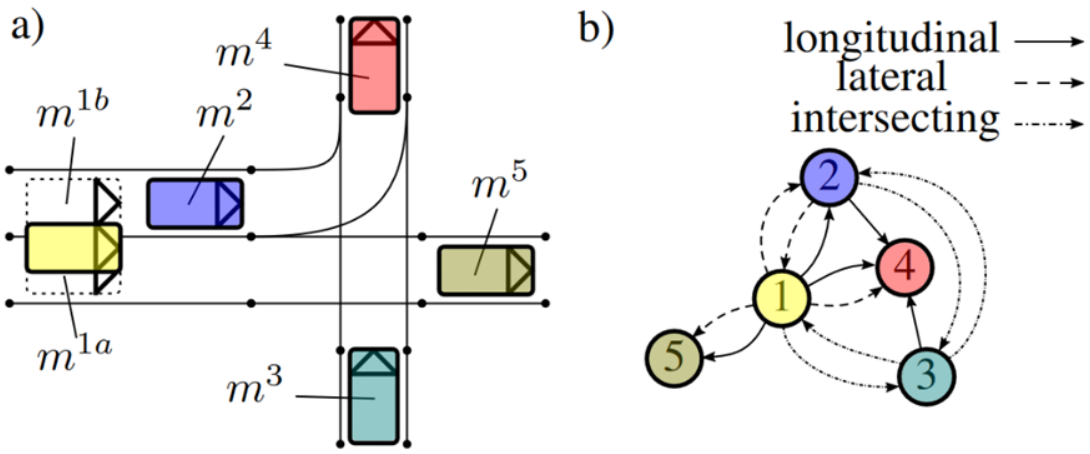


Abbildung 180: a) Beispielhafte Verkehrsszenen mit fünf Fahrzeugen und sechs korrespondierenden Projektionseinheiten m. b) Der resultierende Szenengraph, bei dem jeder Verkehrsteilnehmer als Knoten und die Beziehungen zwischen den Projektionseinheiten als Kanten dargestellt werden [97].

Gruppierung

Die riesige Menge an Daten, die für datengesteuerte Prozesse zur Verfügung steht, ist zweifellos von Vorteil; sie erfordert jedoch auch ein Verfahren, das die Verkehrsszenen zugänglich macht und sie automatisch kategorisiert. Um diese Herausforderung zu meistern, schlagen wir einen kontrastiven Lernansatz vor, der Graphen nutzt, um einen sinnvollen Embedding Space zu konstruieren. Unser Ansatz demonstriert die kontinuierliche Abbildung von Szenen anhand von szenenspezifischen Merkmalen und die Bildung von thematisch ähnlichen Clustern auf der Basis der resultierenden Einbettungen. Basierend auf den gefundenen Clustern können ähnliche Szenen identifiziert werden, die im anschließenden Testprozess weiterverwendet werden [98] [99].

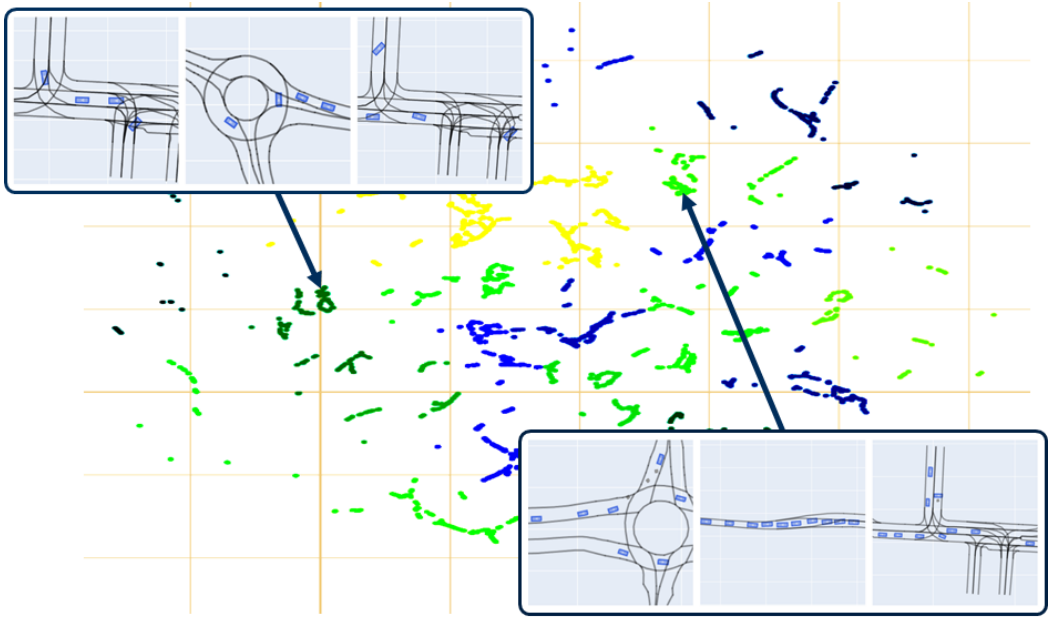


Abbildung 181: Die Dimension des eingebundenen Raums wurde reduziert zu einem zweidimensionalen Raum unter Nutzung des UMAP-Algorithmus [99].

Re-Simulation

Beispielsweise kann mit der Simulationsumgebung "Carla" und verschiedenen (KI-)Verhaltensmodellen aus einer Seed-Szene ein Szenario generiert werden. In dieser Seed-Szene werden die Ausgangsbedingungen festgelegt, u.a. die Anzahl der Verkehrsteilnehmer, deren Positionen und Geschwindigkeiten sowie deren Verhaltenstyp. Bei den für die Verkehrssteuerung verwendeten Verhaltensmodellen handelt es sich entweder um einfache regelbasierte Modelle (z.B. IDM) oder um komplexe maschinengelernte Modelle zur Steuerung anderer Teilnehmer (z.B. [100]).

Ein Szenario, das mit dem zu testenden System (SUT) ausgeführt wird, kann mit traditionellen Kritikalitätsmetriken bewertet werden.

Um die Eignung einer Seed-Szene für die Erstellung eines Testszenarios zu bestimmen, werden viele Kombinationen verschiedener Verhaltensmodelle aller Verkehrsteilnehmer simuliert, anschließend wird ein Profil mithilfe von Kritikalitätsmetriken erstellt [101].

3.1.2.5.2 AP5.2 Verfügbarmachung und Instanziieren einer Simulationsumgebung

Die Hauptaufgabe in AP5.2 bestand darin, die Partner bei der Anwendung der Simulation zu unterstützen. Dies erforderte, dass die Simulation für die Anwender zugänglich gemacht wurde, insbesondere für die Hauptanwendungsgebiete TP2 und TP7. Das TP5 hatte die Aufgabe, diese Teilprojekte auf technischer und methodischer Ebene zu unterstützen. Angesichts der heterogenen Elemente der Simulationslösungen - wie Infrastruktur, Verkehr, Umwelt, Sensorik und Dynamik - sowie der Notwendigkeit, große Verhaltensräume mit gezielten Analysen zu erkunden, stellte die Verwendung der Werkzeuge eine anspruchsvolle Aufgabe dar. Die effiziente Nutzung der Simulation war abhängig von den definierten Zielen, um valide Ergebnisse in angemessener Zeit zu erzielen. Dazu war ein umfassendes Verständnis der Werkzeugverbünde erforderlich, das den Anwendern zunächst fehlte. Eine entscheidende Aufgabe von TP5 bestand darin, sicherzustellen, dass diese technische Anwendungsunterstützung gewährleistet war.

Ein besonderer Schwerpunkt lag dabei auf der Sicherstellung der konsistenten Umsetzung der Anwendung für TP2 und TP7. Ein wesentlicher Aspekt dieser Aufgabe bestand darin, Lösungsvorschläge für auftretende Zielkonflikte unterschiedlicher Anforderungen innerhalb der Anwendung zu erarbeiten.

Basierend auf den Anforderungen aus AP5.1 wurde beschlossen, die Open-Source-Simulationsplattform openPASS für die Kritikalitätsanalyse einzusetzen. In AP5.2 wurde die Anpassung dieser Plattform für die Anwendung in der Kritikalitätsanalyse behandelt. Aufgrund der Mitgliedschaft des TÜV SÜD in der openPASS-Arbeitsgruppe der Eclipse Foundation und der Bereitstellung des Produktmanagers für openPASS durch den TÜV SÜD war es naheliegend, dass der TÜV SÜD die Leitung bei der Instanziierung mit openPASS übernahm.

Um openPASS für die Kritikalitätsanalyse vorzubereiten, waren einige Anpassungen und Erweiterungen erforderlich. Diese wurden im Rahmen eines Unterauftrags (GUA5) mit der Firma in-tech durchgeführt, die einen Entwickler für diese Aufgaben bereitstellte. Der TÜV SÜD übernahm die Verantwortung für das GUA5. Die folgenden Entwicklungen wurden basierend auf den Anforderungen aus AP5.1 umgesetzt:

- Interpretation von Fußgängerüberwegen: Das Simulationstool musste in der Lage sein, Fußgängerüberwege aus einer openDRIVE-Datei zu interpretieren, um das Testszenario im FUC2 zu simulieren.
- Interpretation von Wetterbedingungen: openPASS wurde entsprechend angepasst, um Wetterbedingungen in ein OSI-Format umzuwandeln, damit Modelle diese lesen können.
- Entwicklung eines Fahrradfahrermodells: Ein intelligentes Fahrradfahrermodell wurde entwickelt, das eigenständig eine Trajektorie von einem Startpunkt über den Zebrastreifen zu einem Zielpunkt berechnen und abfahren konnte.
- Entwicklung einer simplen Automatisierungsfunktion: Das GUA5 entwickelte eine einfache Automatisierungsfunktion für Szenario-basiertes Testen, um kritische Situationen zu erkennen und entsprechend zu handeln.
- Bereitstellung eines Ampelsystems: Es wurde ermöglicht, Ampelsysteme in openPASS zu interpretieren, was für die Kritikalitätsanalyse im TP2 essentiell ist.
- Erstellung von Szenarien und Karten: OpenDRIVE- und OpenSCENARIO-Dateien wurden für alle Functional Use Cases erstellt und stehen nun dem gesamten Projekt zur Verfügung.

Alle Entwicklungen im Rahmen der VVMethoden wurden über die Eclipse Foundation der Öffentlichkeit zugänglich gemacht und im openPASS-Repository veröffentlicht. Alle Konsortialpartner stimmten der Veröffentlichung zu.

Für die Auswertung der Simulationsergebnisse wurde das Programm CriSys von ZF verwendet, was eine durchgängige Kette von der Szenarienerzeugung über die Simulation bis hin zur Auswertung ermöglichte.

Eine ausführbare Version von openPASS wurde auf der gemeinsamen Arbeitsplattform Confluence abgelegt. Außerdem wurde es möglich gemacht, die gesamte Simulationskette automatisiert ablaufen zu lassen, angefangen von der Parametervariierung über die Durchführung der Simulation in openPASS bis hin zur Auswertung der Ergebnisse mit CriSys.

Infrastrukturelle Verkehrserfassung für Szenarienextraktion und -analyse

Infrastrukturelle Verkehrsdatenmessung

Die Großforschungsanlagen des DLR ermöglichen es, den realen mikroskopischen Verkehr in vielfältigen Umgebungen kontinuierlich zu erfassen und zu analysieren. Bspw. erlaubt die AIM-Forschungskreuzung in Braunschweig (siehe Abbildung 182 links) die Analyse des Langzeitverkehrs in einem städtischen Umfeld. Darüber hinaus wird die mobile Messstation (siehe Abbildung 182 rechts) zur Untersuchung des kurz- bis mittelfristigen Verkehrs flexibel in verschiedenen Umgebungen eingesetzt. Dabei bilden die erfassten mikroskopischen Verkehrsdaten die Grundlage für die anschließende szenariobasierte Analyse (siehe Abbildung 183).

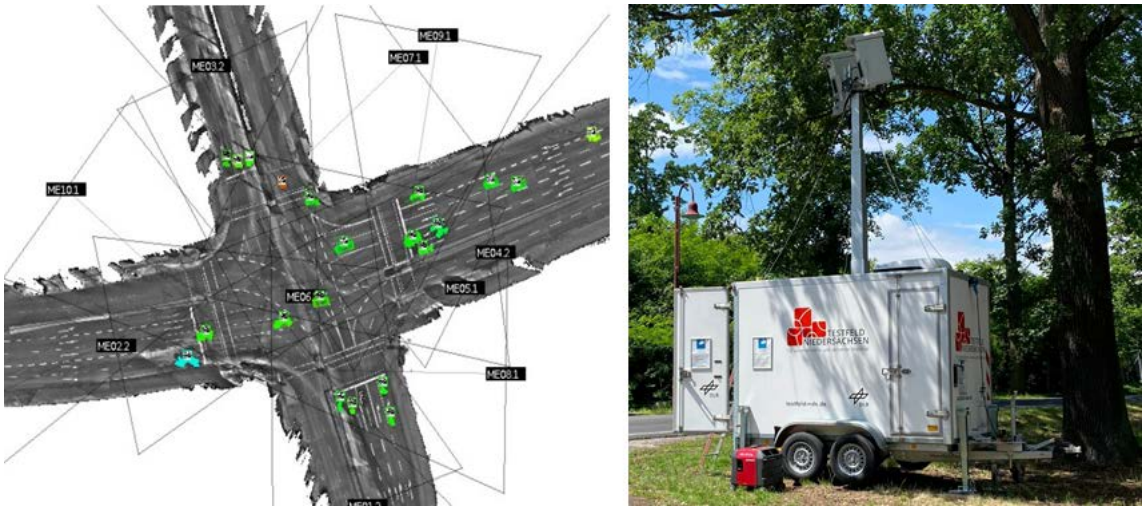


Abbildung 182: Die AIM Forschungskreuzung (links) und der mobile Messanhänger (rechts) für mikroskopische Verkehrsmessungen und die Bereitstellung von konkreten Szenarien (© DLR e.V.).

Scenario Mining Platform

Für das simulationsbasierte Testen von realen, konkreten Szenarien ist es zwingend erforderlich, diese Szenarien in den umfangreichen, von Verkehrsmesssystemen aufgezeichneten, Datensätzen zu finden. Zu diesem Zweck wurde eine modulare und skalierbare Scenario Mining Plattform entwickelt. Sie ist für die Verarbeitung großer Live- und historischer Verkehrsdaten konzipiert. Aufgrund des zugrundeliegenden systematischen Ansatzes zur Identifizierung und Extraktion von Szenarien (auch bekannt als Scenario Mining), ermöglicht die Scenario Mining Plattform den Aufbau eines umfassenden Katalogs von Fahrszenarien.

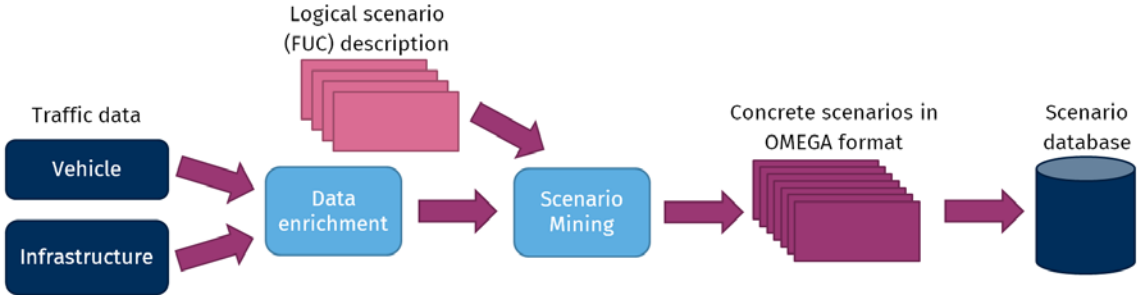


Abbildung 183: Der Gesamtprozess zur Identifizierung und Extraktion konkreter Szenarien aus infrastrukturell erfassten Verkehrsdaten (und Fahrzeugdaten). Die extrahierten Szenarien werden in das OMEGA-Format konvertiert und in der Szenariendatenbank für z.B. simulationsbasierte Analysen gesammelt (© DLR e. V.).

In Anlehnung an das im VVM definierte 6-Schichten-Modell ist ein wichtiger Baustein des gesamten Szenario-Mining-Prozesses die Kategorisierung der Verkehrsteilnehmer nach der von ihnen gewählten Route zum Überqueren von Kreuzungen. Diese Assoziation von Entitäten aus Schicht 1 (Verkehrsteilnehmende) mit Schicht 4 (Straßennetz) ermöglicht nicht nur die Definition von Szenarien wie "ein Fahrzeug, das an einer städtischen Kreuzung links abbiegt, wobei ein entgegenkommendes Fahrzeug die Kreuzung zuerst überquert", sondern ermöglicht auch die Extraktion konkreter Szenarien. Die Szenariendefinition und die infrastrukturell erfassten Verkehrsdaten (und optional der Versuchsfahrzeuge) sind der Input für die Scenario Mining Plattform (siehe Abbildung 183). Diese extrahiert die konkreten Szenarien und konvertiert die

Ergebnisse ins VVM OMEGA-Format, die in der VVM-Szenario-Datenbank für weitere Analysen (zum Beispiel Fahrverhalten, Verkehrssicherheit) und/oder simulationsbasierte Tests gesammelt werden. Ein extrahiertes konkretes Szenario, das der vorangegangenen logischen Szenariodefinition entspricht, ist in Abbildung 184 dargestellt, in der ein Verkehrsteilnehmer (weißes Auto) einen Rotlichtverstoß begeht und ein Vollbremsmanöver durchführt, um eine Kollision mit dem entgegenkommenden Verkehrsstrom zu vermeiden.

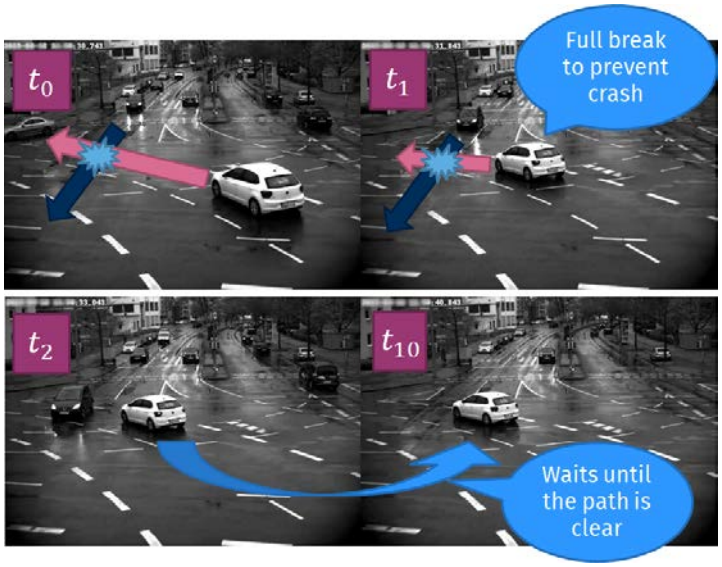


Abbildung 184: Ein automatisch extrahiertes konkretes Szenario auf Basis einer Szenariobeschreibung, in der das linksabbiegende Fahrzeug (weißes Auto) einen Rotlichtverstoß begeht (© DLR e.V.).

3.1.2.6 TP6 Datenbereitsstellung

3.1.2.6.1 HD Kartenerstellung für Ground Truth Daten

Einleitung

Für die szenariengetriebene Entwicklung von ADAS und AD wird die Simulation immer wichtiger [102]. Ground Truth (GT) Karten mit einer globalen Genauigkeit von wenigen Zentimetern gewinnen dabei eine zentrale Bedeutung. Die Erfassung und manuelle Annotieren von realen Szenarien führt zu absoluten und relativen Positionsfehlern. Aufgrund von Fehlerfortpflanzung können GT-Karten und Szenarien nur unzureichend zusammengeführt werden und sind somit für eine realitätsnahe Simulation ungeeignet. Im Folgenden stellen wir einen durchgängigen Prozess von der Datenaufnahme über die Erzeugung der GT-Karten [103] [104] bis zur Re-Simulation vor.

Methodik

Die vorgestellte Methodik besteht aus zwei wesentlichen Schritten, die auf aufgezeichneten realen Szenarien und manuell annotierten Objekten basieren. Dabei werden statische Landmarken wie bspw. Verkehrsschilder verwendet, um die relative und absolute Genauigkeit der generierten Karten als auch der statischen und dynamischen Objekte durch zusätzliche Korrekturalgorithmen zu optimieren. Aus den generierten Daten werden nahezu automatisch re-simulierbare Szenarien erzeugt.

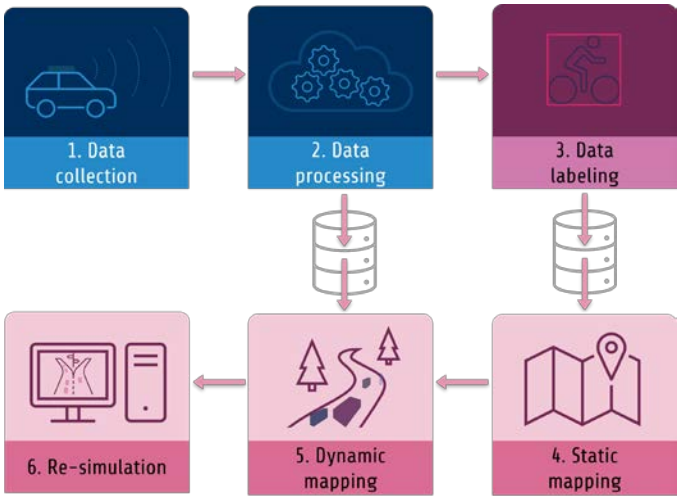


Abbildung 185: Schematischer Überblick über den Gesamtprozess der Kartenerstellung und Szenarienrekonstruktion.

Statische Kartierung

Hochgenaue georeferenzierte Bilder und reale Messungen werden zur Erstellung von GT-Karten verwendet. Durch pixelgenaues Annotieren der georeferenzierten Bilder werden Straßenmarkierungen und Objekte wie Verkehrsschilder in Weltkoordinaten abgebildet und mit ihren syntaktischen Informationen in Fahrspuren und Kreuzungen übertragen. Darüber hinaus liefern sorgfältig ausgewählte hochgenaue Messungen globale Offset-Korrekturen. Die GT-Karten werden in den OpenDRIVE-Standard exportiert.

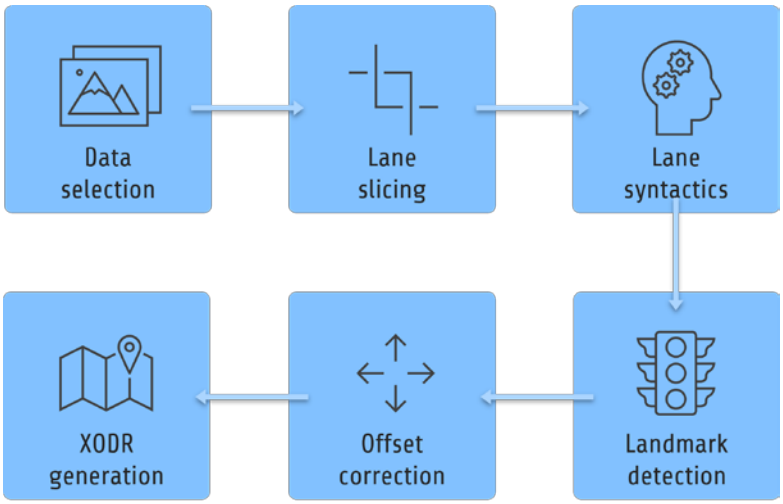


Abbildung 186: Schematischer Prozess der statischen Kartenerstellung, beginnend mit der manuellen Datenauswahl entsprechend dem gegebenen Szenario.

Dynamisches Mapping

Anhand der manuell annotierten Objektdaten werden die Trajektorien für jedes Objekt extrahiert und optimiert. Jedes Objekt wird dabei durch seine globalen Koordinaten (World Geodetic System 1984, WGS84) beschrieben. Die resultierenden Trajektorien werden mit dem RTK-GNSS des Fahrzeugs optimiert und durch statischen Landmarken global korrigiert. Anschließend werden die Trajektorien weiter gefiltert und auf die GT-Karte projiziert, um die statische Welt mit den dynamischen Objekten zu kombinieren.

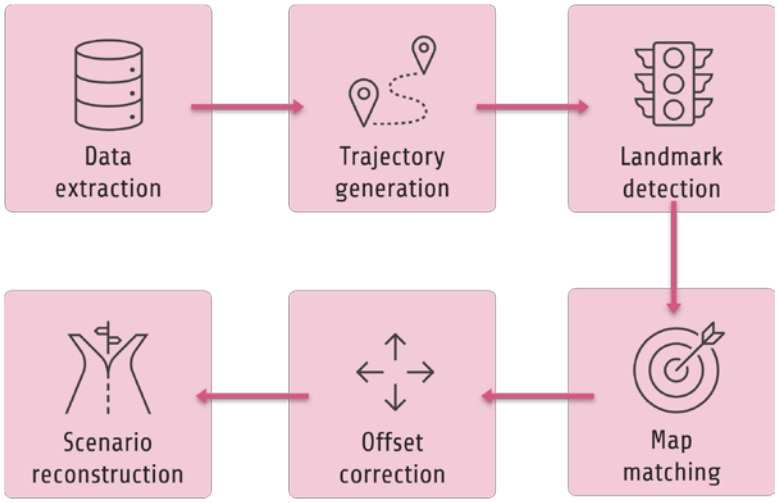


Abbildung 3: Überblick über den dynamischen Mapping-Prozess . Auf der Grundlage der bereitgestellten Daten werden Objekttrajektorien extrahiert, global kartiert und mit Hilfe eines landmarkenbasierten Optimierungsprozesses korrigiert.

Demonstration

Nachfolgend ist die simulierte Welt als Überlagerung auf einer reellen Fahrzeugmessung dargestellt.

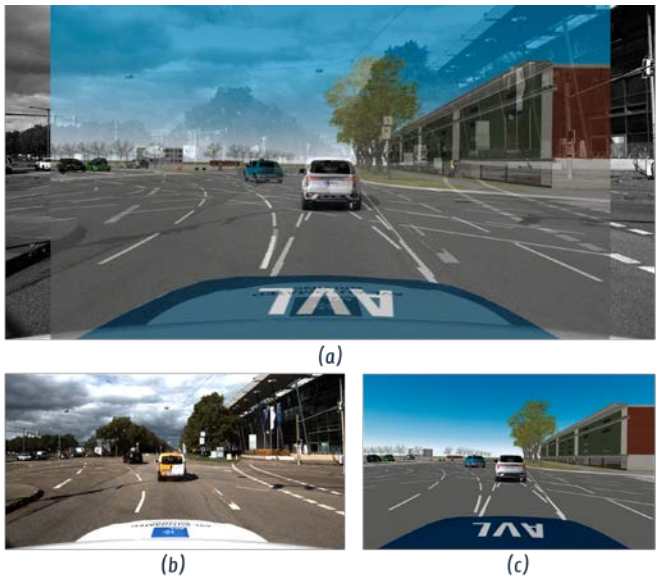


Abbildung 187: Projektion (a) der generierten GT-Karte und des dynamischen Szenarios (c) auf reale Daten (b). CarMaker wird für die Simulation verwendet.

3.1.2.6.2 Datenreduktion

Motivation

- ADS erzeugen große Datenmengen
- Die Beschränkung der Daten auf die für die Bearbeitung relevanten Informationen ist essentiell

Schritt 1: Relevanz definieren

Relevanz ist von Natur aus mit einem Subjekt und einer Aufgabe verbunden. Daher muss jede Definition von Relevanz beide Komponenten berücksichtigen. Stuctured Analysis for Conservative Relevance Estimation in Driving context (SACRED) [105], wie in Abbildung 188 dargestellt, ist eine Methode zur Ableitung einer konservativen Schätzung für das automatisierte Fahren. Das zugrundeliegende Konzept für das, was relevant ist, lautet: "Alle Objekte, die die Menge der möglichen Trajektorien verändern können, sind relevant für die Lösung der kombinierten Planungs-/Wahrnehmungsaufgabe."

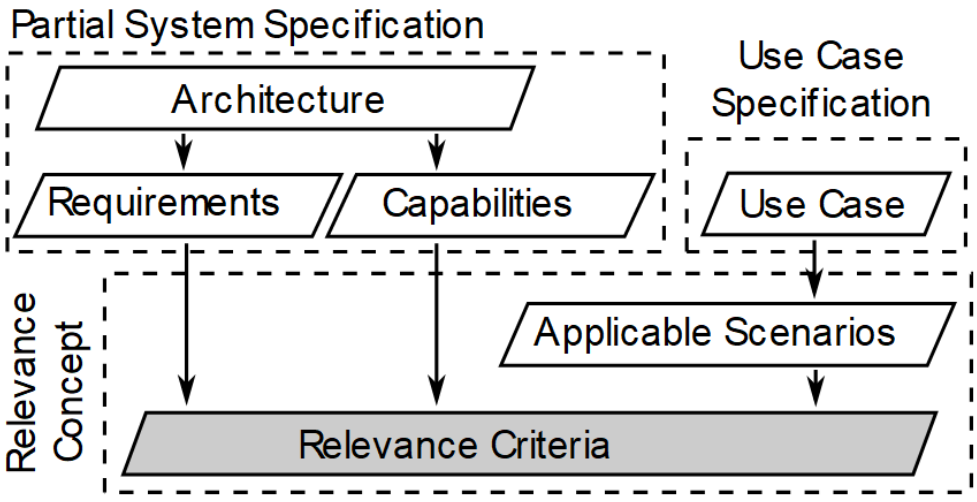


Abbildung 188: SACRED Methode (© TU Darmstadt)

Schritt 2: Relevanz identifizieren

Als Relevanzkriterien schlägt SACRED sechs Basisszenarien für den urbanen Anwendungsfall mit entsprechenden planerunabhängigen Kriterien vor. Die Kriterien beruhen auf gesetzlichen Vorgaben und Worst-Case-Annahmen. Alle anwendbaren Szenarien werden überlagert und bewerten paarweise radiale und tangentiale Wechselwirkungen [105] [106] (siehe Abbildung 189).

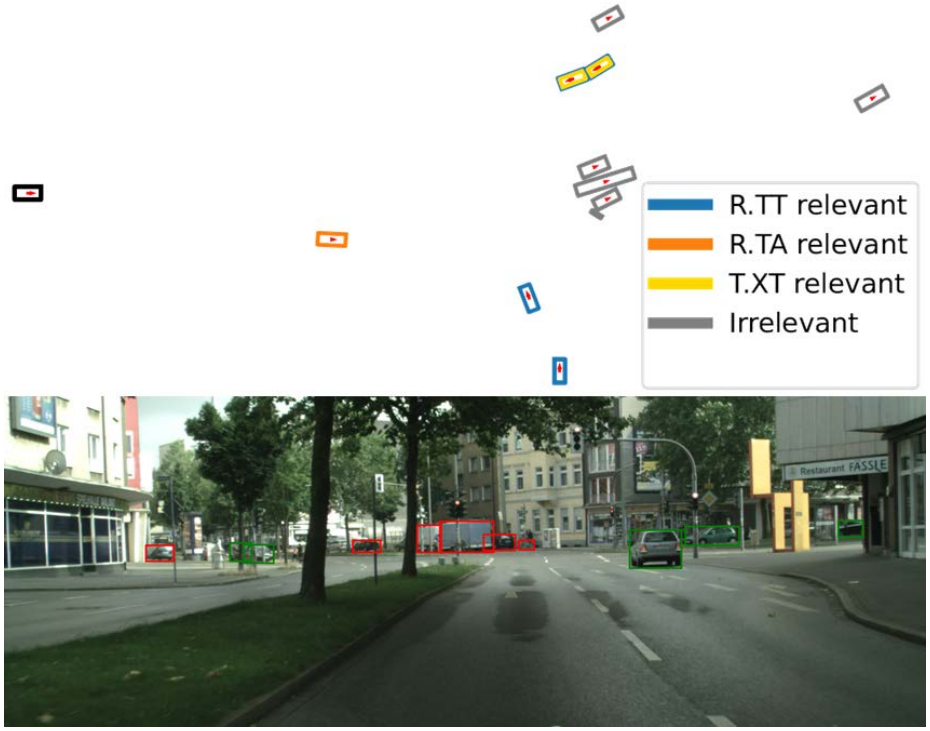


Abbildung 189: Erkannte potentiell relevante Fahrzeuge in der Vogelperspektive mit entsprechenden Kriterien und in der Ego-Ansicht (© Cityscapes Dataset | TU Darmstadt)

Schritt 3: Relevanz validieren

Die Validierung eines Relevanzkonzepts ist unerlässlich, bevor es zur Datenreduktion verwendet wird. Zu diesem Zweck bietet SURE-VAL [106] eine Strategie zur Validierung von Relevanzkonzepten gegenüber einer bekannten Referenz auf der Grundlage ihres Aufgabeneinflusses.

Schritt 4: Daten reduzieren

Die kontextbewusste Datenreduktion (Context Aware Data Reduction, CADR) ist eine aufgabenorientierte Methode zur iterativen Datenreduktion, bei der festgelegt wird, welche Objekte in einer Szene relevant sind. Relevante Entitäten bleiben mit ihren ursprünglichen Daten erhalten, während irrelevante Entitäten aus einer reduzierten Darstellung synthetisiert werden, um eine "plausible Lüge" für den Anwendungsfall zu bilden. Abbildung 190 zeigt eine Beispielanwendung, die auf semantischen Merkmalen für die Reduktion und Generative Adversarial Networks (GAN) für die Synthese basiert.

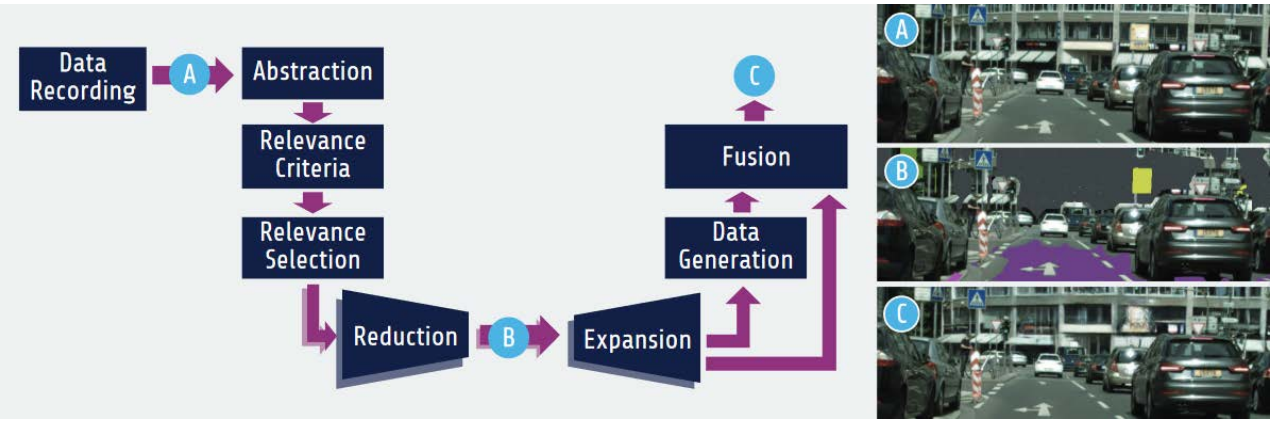


Abbildung 190: Links: Verfahren zur kontextbewussten Datenreduktion mit vorgeschalteter Relevanzerkennung. Rechts: A: Ursprüngliches Eingabebild, B: Reduziertes gespeichertes Bild, C: Teilweise synthetisiertes Bild (Links © TU Darmstadt, rechts © Cityscapes Dataset | TU Darmstadt)

3.1.2.6.3 Datenaufzeichnungsprozess

Workflow Datenerfassung

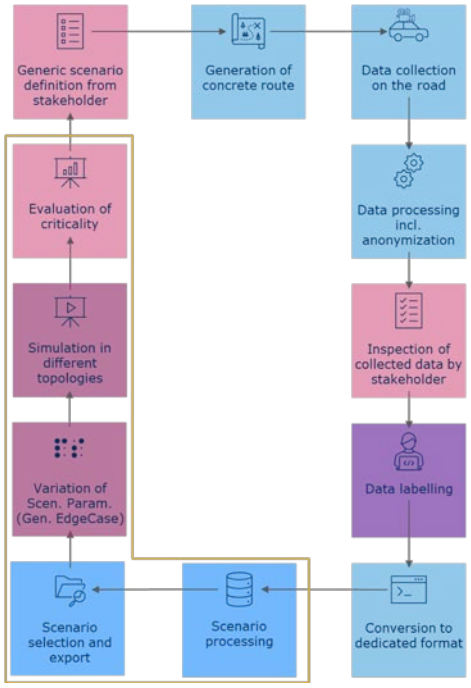


Abbildung 191: Datenerfassung Workflow

Generisches Szenario von Stakeholdern

Die Functional Use Cases für das VVM-Projekt kombiniert mit dem Criticality-Phänomen dienen als Basisanforderungen für die Datenerfassung.

Abbildung 192: Beispiel Functional Use-Case

Routen-Generierung

Das AVL-Tool JUNCEL wird für die Suche nach Kreuzungen in der realen Welt verwendet, die im Projekt definiert sind. Es hilft bei der Suche nach Kreuzungen mit verschiedenen Eigenschaften und Suchkriterien, z.B. Unfallinformationen aus dem deutschen "Unfallatlas".

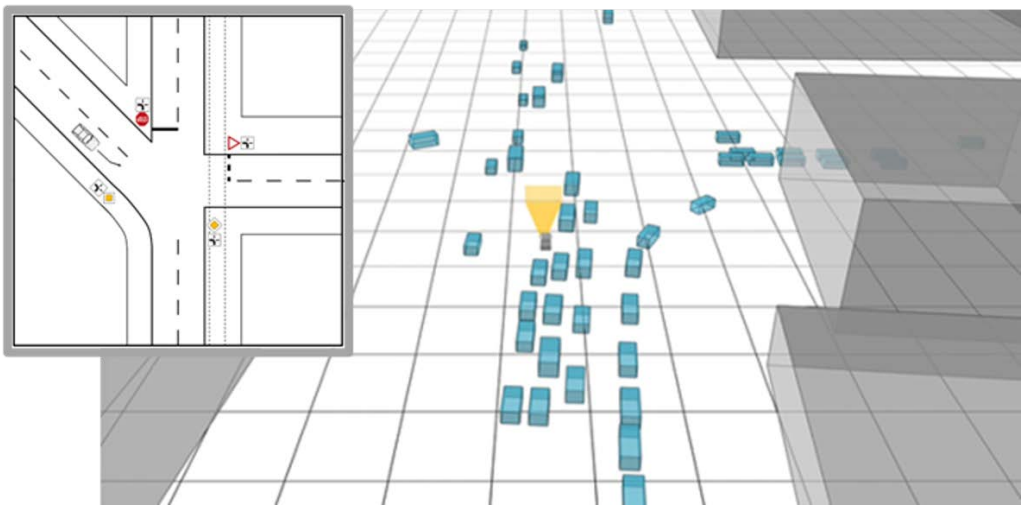


Abbildung 193: JUNCEL - Kreuzungssuche mit verschiedenen Filterkriterien

Real Welt Datenerfassung

Sensor-Datenerfassung:

Synchronisierte Datenerfassung des Referenzsensorsystems und des Sensor-under-Test an den ausgewählten Kreuzungen.

Abbildung 194: Referenzsensor-System Live-Viewer(links). Referenz Sensor System Setup (oben rechts), Sensor unter Test (unten rechts).

Digital Logbuch:

Das AVL Digital Logbuch hilft kritische Situationen bei der Aufzeichnung zu protokollieren.

Abbildung 195: Digitales Logbuch mit Tags für kritische Situationen

Datenverarbeitung inkl. Anonymisierung

Die erfassten Daten werden in einer Rohdatenbank (RAW DB) gespeichert, verarbeitet und gemäß GDPR anonymisiert. Der Lesezugriff, der Ingest von Labeldaten und die Konvertierung in verschiedene Formate erfolgen innerhalb der RAW-DB.

Szenario-Auswahl

Für die Weiterverarbeitung wird eine Vorauswahl anhand der Anforderungen getroffen. Um das Szenario auszuwählen und zu filtern, wird ein zweistufiges Konzept verwendet.

- AVL filtert Szenarien auf der Basis von Kritikalitäts-Tags, Wetter, GPS-Informationen, etc.

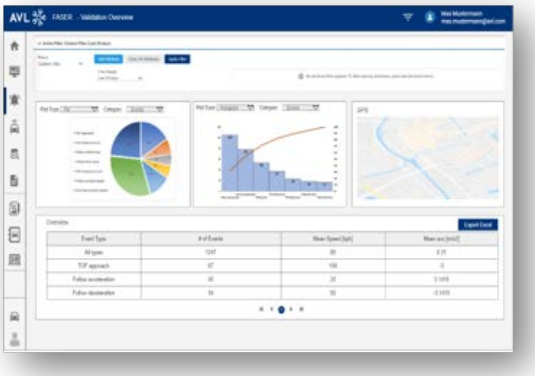


Abbildung 196: Auswählen von Daten anhand von Kritikalitäts-Tags

- Projektpartner analysieren die anonymisierten Preview-Videos

Abbildung 197: Anonymisierte Videos für die visuelle Datenauswahl

3.1.2.6.4 Durchgängiges Beispiel

Integration von Testobjekten in den "VV-Methode"-Prozess

Zur Demonstration der Szenarioverarbeitung in verschiedenen Testeinheiten auf der Grundlage der erfassten Realweltdaten wird der in Abbildung 198 dargestellte Arbeitsablauf verwendet. Die erfassten Daten werden z.B. verwendet, um ein gewisses Vertrauen für die im Projekt getroffenen Annahmen zu erhalten.

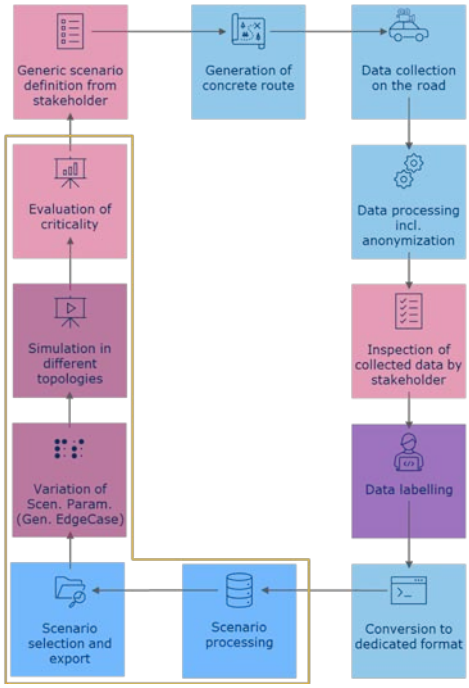


Abbildung 198: Arbeitsablauf der Datenerfassung

Datenerfassung auf der Straße

Testfahrzeug für die parallele Erfassung von Dynamic Ground Truth (DGT): Referenzsensorik auf dem Dachgepäckträger Sensor unter Test (SeUT): Erweiterte Sensorik im Fahrzeug

Abbildung 2: Testfahrzeug in einem realen Szenario

Datenbank-Lösung

- Anonymisierte Kamerabilder und Punktwolken: durch Labelling aus der Rohdatenbank gezogen
- Objektlisten: werden von Labelling in die Eingabedatenbank übertragen

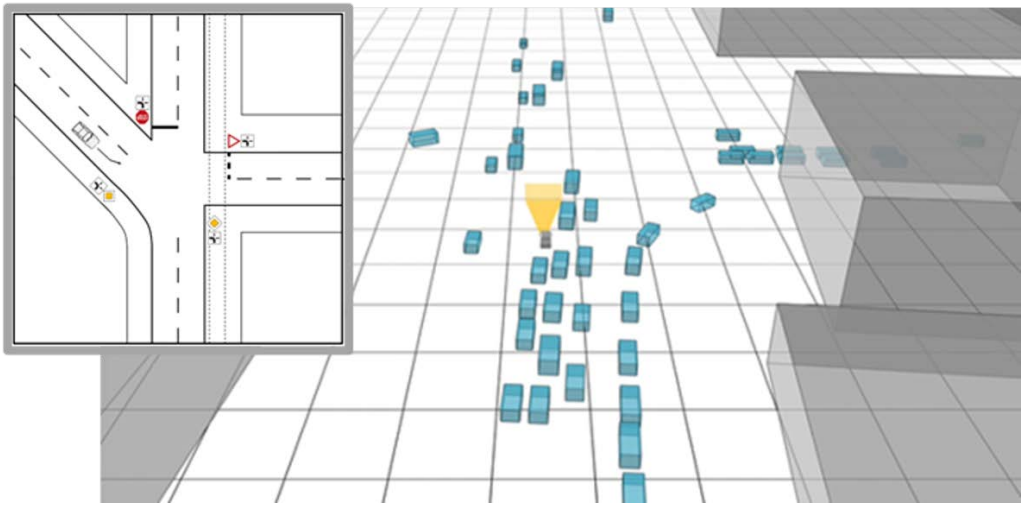


Abbildung 199: Eingangsdatenbank für Scenario Engine

Verarbeitung, Auswahl und Export von Szenarien

- Szenario-Identifikation
- Abstraktion und Interpretation zu Attributen und Parametern
- Semantische Dekomposition
- Auswahl der relevanten Szenarien

Abbildung 200: Konkreter Testfall in virtueller Testumgebung

Simulation mit verschiedenen Topologien

- Testfall-Zusammenstellung
- Eingaben Logisches Szenario und Parameterverteilung
- Outputs Testdaten für SiL, XiL, Proving Ground

Abbildung 5: Vehicle-in-the-Loop-Tests

3.1.2.7 TP7 Testvorgehen

Die Gesamtmethode bietet eine Darstellung der Prozesse, die von der Konzeption bis zur Freigabe eines technischen Systems notwendig sind. Als zentrales Ergebnis von VVM beantwortet es die Frage, was getan werden muss, um ein marktreifes ADS Level 4/5 zu entwickeln. Über die einzelnen Prozessschritte hinaus enthält die Übersicht aber auch deren wesentliche Verknüpfungen, die die logische inhaltliche Abhängigkeit der einzelnen Schritte widerspiegeln. Aus Gründen der Übersichtlichkeit werden diese Abhängigkeiten im Verlauf nur vorwärts dargestellt, d.h. Iterationsschleifen und Rückkopplungen an den Schnittstellen sind natürlich vorhanden, aber nicht gesondert abgebildet.

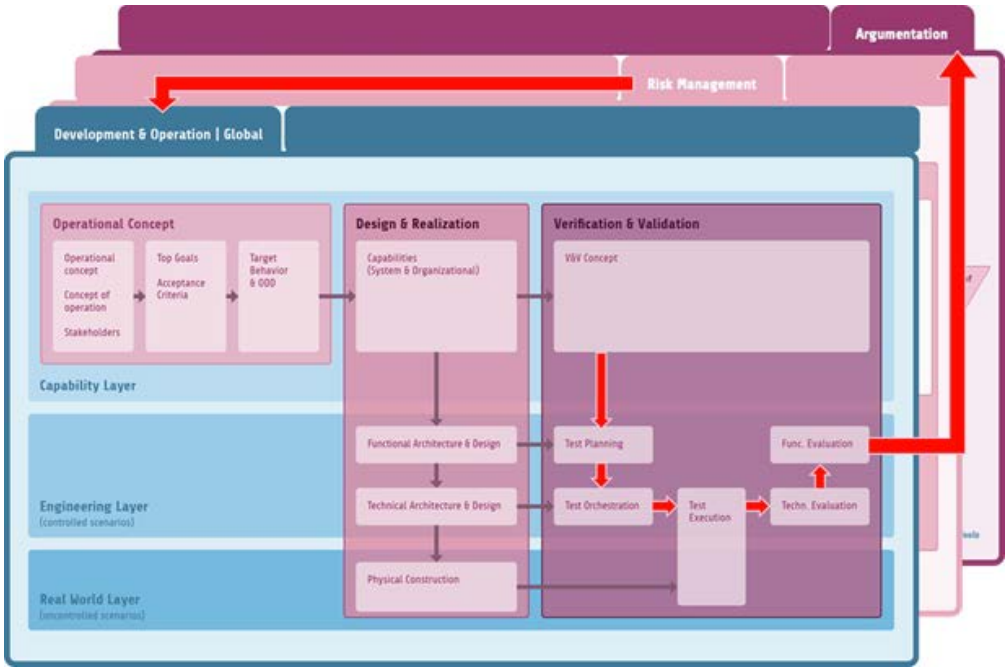


Abbildung 201: V&V in der Gesamtmethodik

Die globale Perspektive Development & Operation der Gesamtmethodik zeigt die Kernprozesse des TP7 bestehend aus der Testorchestrierung, Testdurchführung sowie Testauswertung innerhalb des V&V Teils. Es bestehen wichtige Verbindungen zu den Perspektiven des

Risikomanagements und der Argumentation. Das Risikomanagement liefert das Risikomodell als Voraussetzung für den Designprozess und für die Aggregation der Ergebnisse innerhalb der funktionalen Evaluation. Die Argumentation ist der Adressat der Bewertungsergebnisse. Gemäß dem Konzept der Unterteilung in funktionale und technische Ebene folgt die Testorchestrierung auf die Testplanung und ist abhängig vom technischen Entwurf.

3.1.2.7.1 Testprozess

3.1.2.7.1.1 Testorchestrierung

Die Testorchestrierung muss die Verbindung zwischen der Testplanung einerseits und der Testdurchführung andererseits herstellen. Sie trägt damit dazu bei, dass die Sicherheitsargumentation bei der Umsetzung des V&V-Konzeptes vollständig durchgeführt werden kann. Dabei muss sie stets die Themen effizientes Testen, Durchführbarkeit, Signifikanz und Abdeckung des Testraums im Auge behalten. Konkret geht es bei der Testorchestrierung darum, die funktionalen Testspezifikationen in technische Testspezifikationen zu übersetzen. Der wesentliche Unterschied ist der Übergang von der Betrachtung lösungsneutraler Funktionen zur Betrachtung der realen Welt der implementierten und existierenden Testobjekte und -instanzen. Analog zur funktionalen Testspezifikation enthält eine technische Testspezifikation alle detaillierten Testanforderungen, die in diesem Fall für die konkrete Durchführung eines einzelnen Testfalls oder einer Gruppe gleichartiger Testfälle benötigt werden. Wesentliche Aspekte sind die Definition des Testobjekts (z.B. Komponenten, Baugruppen, Subsysteme oder das Gesamtsystem), die Auswahl der Testinstanz (z.B. SiL, HiL, Prüfstand, Prüfgelände oder Feld) einschließlich der Beschreibung des Testszenarios und die Beschreibung der Testziele, die die konkret zu untersuchenden Messgrößen enthalten.

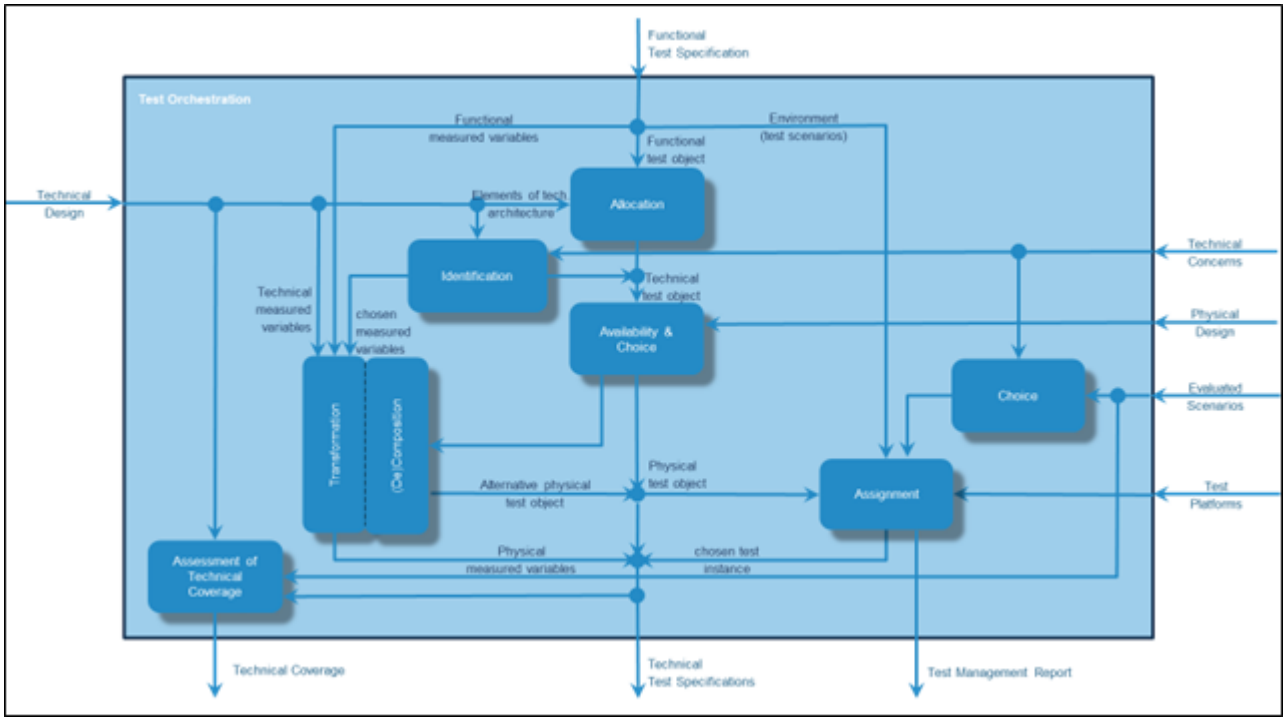


Abbildung 202: Testorchestrierung Detailprozess

Die Kernprozesse sowie Ein- und Ausgänge der Testorchestrierung sind in Abbildung 202 dargestellt. Im Gesamtprozess der VV-Methoden stellt die technische Testspezifikation (TT), das Austauschdokument zwischen Testorchestrierung und Testdurchführung dar. Die TT fungiert somit

als Kommunikationslinie zwischen Testmanagern und Testingenieuren. Mit dem Format und der Umsetzung der TT werden hohe Ziele verfolgt. Zum einen soll es die Konsistenz der Sicherheitsargumentation über die Testplattformen SiL, HiL, Testgelände und Realverkehr hinweg ermöglichen. Im Hinblick auf die Testautomatisierung muss der TT daher zumindest teilweise sowohl von Menschen als auch von Maschinen lesbar und interpretierbar sein. Diese Durchdringung öffnet die Tore für eine Neuausrichtung der notwendigen Tests für V&V. Die Tests verlagern sich von kostspieligen und zeitintensiven Tests, wie z. B. im realen Straßenverkehr, hin zum massiven Einsatz von SiL, insbesondere von ganzheitlichen Simulationen der Wahrnehmung, Bewegungsplanung und Betätigung in realen Umgebungen. Auf der anderen Seite muss sich das TT in eine lange Geschichte verschiedener Formate und Konzepte zur Testbeschreibung einreihen, die von verschiedenen Projektpartnern, aus früheren Forschungsprojekten wie dem PEGASUS-Projekt und aus bestehenden Standards und Normen wie ISTQB®, OSI, FMU, OpenX stammen.

Der TT muss für verschiedene Arten von Prüfungen anwendbar sein:

- Komponenten- und Systemtests
- Szenariobasierte und nicht-szenariobasierte Tests
- Open-Loop- und Closed-Loop-Tests

Vor diesem Hintergrund haben wir einen Vorschlag für das Format des TT erarbeitet und exemplarisch auf den vier Testplattformen erfolgreich angewendet. In verschiedenen multilateralen Diskussionsgruppen wurden für VV-Methoden folgende Paradigmen für die Erstellung der TT entwickelt:

- Die Testingenieure müssen allein durch die TT bereits über ausreichende Informationen verfügen, um einen Test mit einem vordefinierten Testziel durchzuführen.
- Der TT beschreibt nur eine Testinstanz, da ein Ingenieur typischerweise nur in einer Testinstanz über Expertise verfügt. Für direkte Vergleichsmessungen verschiedener Testinstanzen, wie z. B. eine Simulation in SiL und ein Test im realen Verkehr, sind zwei analoge TTs zu erstellen.
- Der TT enthält mindestens einen Testfall, der durch festgelegte Variationsregeln aus der funktionalen Testspezifikation auf bis zu N Testfälle erweitert werden kann. Jeder einzelne Testfall liefert dann Messdaten, die in der Testauswertung gemeinsam ausgewertet werden können.
- Die Testauswertung ist grundsätzlich Teil der TT und sollte die Testziele widerspiegeln.
- Prinzipiell können einzelne Felder in bestimmten TT leer bleiben. Dies ermöglicht diverse Ableitungen des TTs in einem Format.

Um die Anforderung der Maschinenlesbarkeit zu erfüllen, schlagen wir ein JSON-Format (JavaScript Object Notation) vor, das bereits von einzelnen Projektpartnern zur Beschreibung von Tests verwendet wird. JSON ist ein offenes Standard-Dateiformat und Datenaustauschformat, das menschenlesbaren Text zur Speicherung und Übertragung von Datenobjekten verwendet. Es ist ein weit verbreitetes Datenformat mit vielfältigen Anwendungen im elektronischen Datenaustausch, einschließlich Webanwendungen mit Servern. Daher ist es ein vielversprechender Kandidat für die

zukünftige Anbindung an die verschiedenen Schnittstellen aktueller und zukünftiger Testinstanzen.

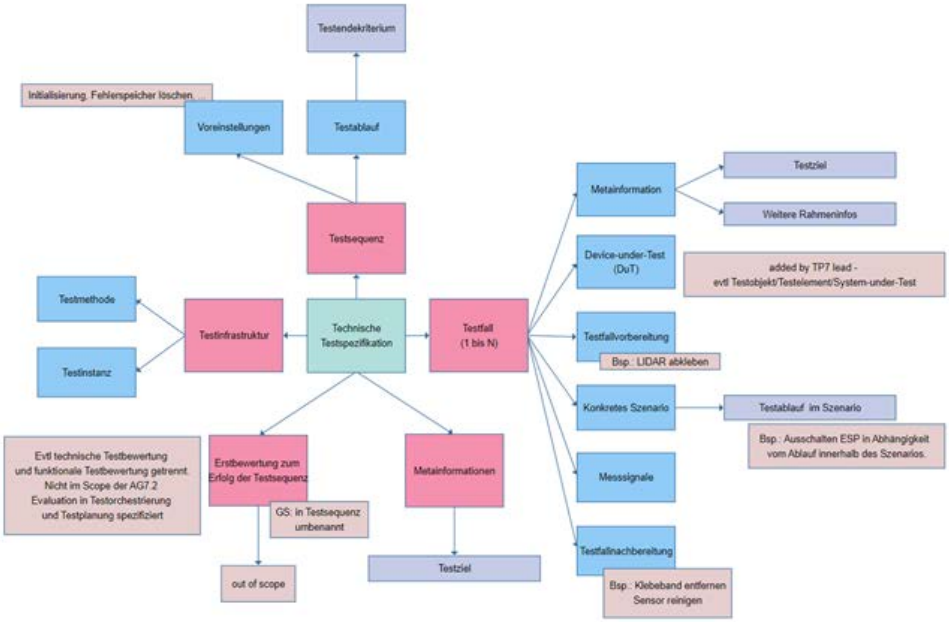


Abbildung 203: Hierarchische Darstellung der Kapitel der technischen Prüfspezifikation.

Die Struktur des TT ist in Abbildung 203 entsprechend dem Stand der Arbeiten dargestellt. Sie gliedert sich in fünf Hauptkapitel: Metainformation, Testfall, Testinfrastruktur, Testablauf und Erste Bewertung des Erfolgs des Testablaufs. Den Hauptkapiteln (rote Kästen) sind bis zu zwei weitere Ebenen von Unterkapiteln zugeordnet. Die Auswertung von Testdaten und die Erstellung von gesammelten Ergebnissen eines Tests wird im TT explizit nicht beschrieben.

Metainformationen

In diesem Kapitel werden Metainformationen für den gesamten TT gespeichert. Dies ist z.B. das Testziel für den gesamten TT oder auch die Änderungshistorie des Dokuments.

Testfall

Der Testfall stellt einen einzelnen, ausführbaren Test mit statischen und dynamischen Szenarien dar. Der Testfall enthält folgende Unterabschnitte

1. Metainformationen: Enthält zusätzliche Informationen für den Testingenieur, wie z.B. das Testziel.
2. Konkretes Szenario: Abgeleitet von logischen Szenarien, wie sie im PEGASUS-Projekt definiert wurden.
3. Zu prüfendes Gerät (DuT).
4. Testfallvorbereitung: Erste Vorbereitungen vor dem Start eines einzelnen Testfalls.
5. Gemessene Signale: Liste der aufzuzeichnenden Signale wie Fahrzeugsignale oder externe Referenzsignale (z. B. Time-to-Collision).

6. Nachbereitung des Testfalls: Verfahren, das nach dem Test durchgeführt werden muss, zum Beispiel das Versetzen der Testinstanz in den Ausgangszustand.

Das erste Unterkapitel "Metainformation" mit dem Testziel für einen einzelnen Testfall und das zweite Unterkapitel "Konkretes Szenario" gemäß der Definition aus dem PEGASUS-Projekt bilden die Kernpunkte des Testfalls.

Test-Infrastruktur

Die Testinfrastruktur beschreibt die Testausrüstung mit Hardware und Software, die nicht vom einzelnen Testfall abhängt. Die Testinfrastruktur umfasst die folgenden Unterabschnitte

1. Konfiguration der Testinstanz: Konkrete Beschreibung der (minimalen) Hardware und (minimalen) Software, z.B. Modelle, der Testgeräte zur Testdurchführung.

2. Testdaten-Management: Hinweise zur Speicherung der Testdaten.

Das Hauptaugenmerk liegt auf dem Testset, das die benötigten Artefakte, insbesondere konkrete Hard- und Software, mit entsprechenden Versionsnummern für die erforderliche Rückverfolgbarkeit detailliert beschreibt. Die Parameter zur Durchführung von Tests an einer Testinstanz werden im Unterkapitel "Testfall" vorgestellt.

Testablauf

Die Testsequenz enthält die Vorgabe für die Durchführung der einzelnen Testfälle. Die Testsequenz enthält folgende Unterabschnitte

1. Vorbereitung des Testablaufs: Grundeinstellungen für die Durchführung der Testsequenz.

2. Testablauf: Ablaufbeschreibung für die Ausführung der einzelnen Testfälle. Seriell oder parallel sind hier die Optionen.

Entscheidend ist hier die Testsequenz, die jeden Schritt zur Durchführung des Tests für die Testingenieure detailliert beschreibt. Für die automatisierte Ausführung ist dieser Abschnitt zumindest teilweise maschinenlesbar.

Erste Bewertung des Erfolgs der Testsequenz

In diesem Kapitel wird eine erste Plausibilitätsprüfung des Tests durch den Testingenieur erläutert. Ziel dieses Verfahrens ist es, grobe Fehler in der Testdurchführung frühzeitig zu erkennen. Es wird keine vollständige Auswertung der Tests beschrieben.

3.1.2.7.1.2 Testausführung

Durch die Bereitstellung technischer Testspezifikationen ermöglicht die Testorchestrierung durchgängiges Testen, d.h. die Realisierung von Komplementarität, Effizienz, Wiederverwendbarkeit, Konsistenz und Flexibilität bei der Testdurchführung.

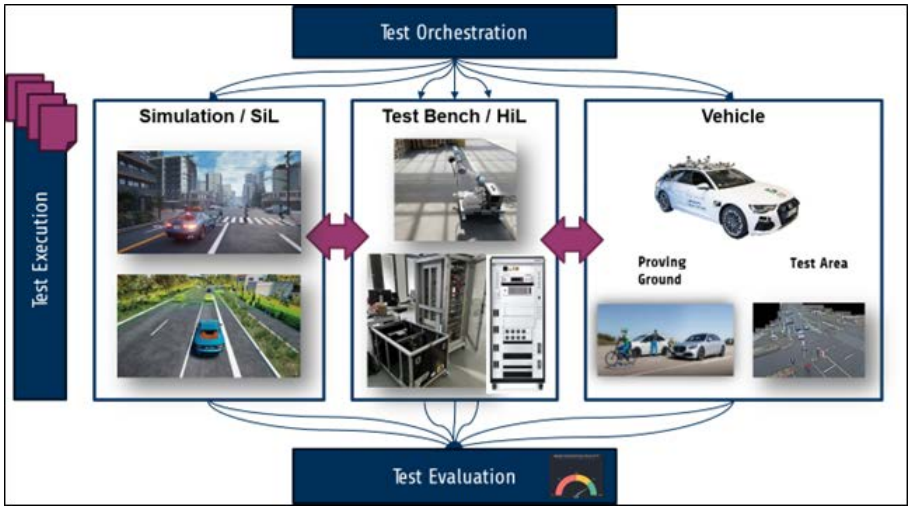


Abbildung 204: Durchgängiges Testen

3.1.2.7.1.3 Testauswertung

In Anlehnung an das zweistufige Verfahren zur funktionalen und technischen Planung von Tests wird auch die Auswertung in einen funktionalen und einen technischen Schritt unterteilt (siehe Abbildung 205). Die technische Auswertung entspricht der Testorchestrierung. Auf dieser Ebene werden die bei der Durchführung der Tests erzeugten Testdaten technisch ausgewertet. Da die technischen Schnittstellen und Signale nicht notwendigerweise den funktionalen entsprechen, ist auch eine Rücktransformation der technischen Messwerte in funktionale notwendig, analog zum Schritt von der funktionalen zur technischen Spezifikation. Somit wird der Ansatz der Architektur-, Design- und Testplanung zur Trennung von funktionalen und technischen Aspekten mit all seinen Vorteilen auch bei der Auswertung konsequent verfolgt.

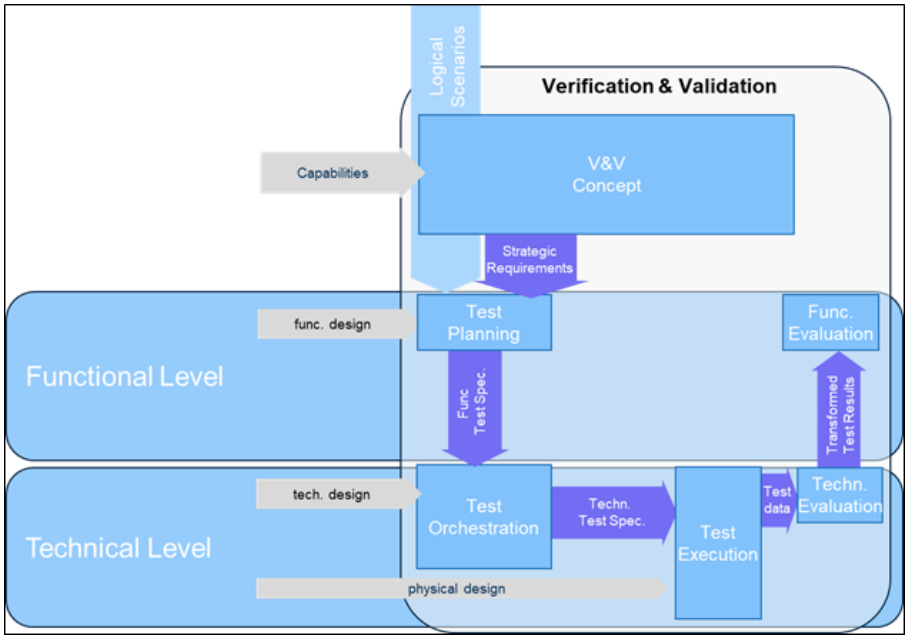


Abbildung 205: Technische und Funktionale Auswertung in VVM.

Bis zu diesem Punkt beschäftigt sich die beschriebene Auswertung noch mit einzelnen Testfällen. Diese Testfälle sind aus der Zerlegung in drei Richtungen entstanden:

- Testobjekt: Produktsystem → Komponenten
- Testbetriebsumgebung: ODD → Szenarien
- Testziele: Oberstes Sicherheitsziel → Sicherheitsunterziele

Das endgültige Ziel ist eine ganzheitliche Aussage zur Sicherheit, d.h. vollständig in Bezug auf das Produkt, seine Einsatzumgebung und die verfolgten Sicherheitsziele. Kurzum, die einzelnen Teilergebnisse der zerlegten Testfälle müssen dann wieder zu einem Gesamtergebnis zusammengeführt werden. Abbildung 206 zeigt ein Beispiel für die Herausforderung der Aggregation mehrerer funktionaler Ergebnisse. Mit anderen Worten: Die einzelnen Unsicherheitsbeiträge werden über die Summe der Komponenten, Szenarien und Sicherheitsziele "aufaddiert". Dies geschieht in einem Aggregationsschritt innerhalb der Funktionalen Bewertung. Für die Konsolidierung der Bewertung wird dasselbe Modell verwendet, nach dem die Sicherheitsanforderungen zuvor in Komponenten, Szenarien und Unterziele aufgeteilt wurden und das sich im Block "Risikomanagement" des Assurance Framework befindet.

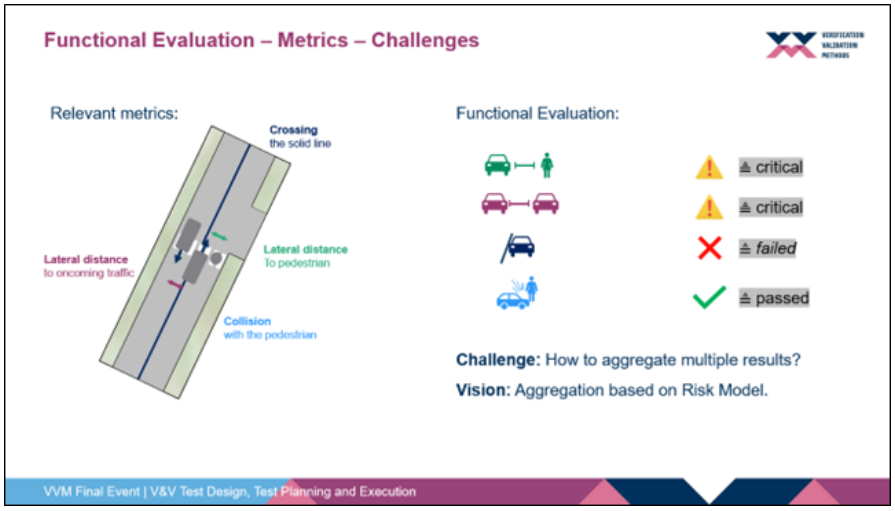


Abbildung 206: Beispiel für mehrere Ergebnisse und die Herausforderung der Aggregation.

Damit liefert die konsolidierte Bewertung einen wesentlichen Teil der Argumentation, nämlich den objektiven Nachweis für das Systemverhalten des ADS-Produkts, der sich aus der Anwendung der Methoden in den miteinander verknüpften Prozessschritten ergibt.

3.1.2.7.2 Durchgängiges Testen

Der Begriff des durchgängigen Testens umfasst die ergänzende Argumentation auf der Grundlage des im ersten Kapitel vorgestellten Testprozesses. Dies soll auch durch die nahtlose Nutzung verschiedener Testplattformen unterstützt werden. Die folgenden Schlüsselthemen in Bezug auf nahtloses Testen werden angesprochen:

- Vertikale Aspekte: Nahtloses Testen soll eine komplementäre Argumentation ermöglichen, die von der Testorchestrierung über die Testdurchführung bis zur Testauswertung reicht, wie in Abbildung 205 dargestellt. Dies beinhaltet eine Aufschlüsselung von funktionalem Design und funktionalem Testen zu technischem Design und technischer Testspezifikation. Die Testdurchführung erfolgt parallel auf verschiedenen Testplattformen und nach verschiedenen technischen Testspezifikationen. Anschließend muss eine Bewertung jedes Tests auf der Grundlage verschiedener Metriken erfolgen, die von den entsprechenden

System-KPIs abgeleitet werden. Zusätzlich müssen alle einzelnen Testergebnisse im Hinblick auf die gesamte Sicherheitsargumentation harmonisiert werden. Der nahtlose Ansatz sollte eine harmonisierte und nachvollziehbare

- Horizontale Aspekte: Für die Durchführung von Tests auf technischer Ebene stehen unterschiedliche Testplattformen zur Verfügung. Dies reicht von der Simulation in einer virtuellen Umgebung über X-in-the-Loop-Ansätze auf einer halbvirtuellen Ebene bis hin zu Fahrzeugtests in der realen Welt, die auf Testgeländen oder öffentlichen Versuchsflächen durchgeführt werden können.

Abbildung 207: Verschiedene Testplattformen und deren nahtlose Nutzung

Die Testplattformen, dargestellt in Abbildung 207, sollten komplementär und durchgängig genutzt werden. Ein Beispiel ist die nahtlose Testdurchführung bestimmter Tests oder Szenarien auf verschiedenen Testplattformen, indem dieselbe Szenariobeschreibung, dieselben Modelle oder dieselben Metriken / KPIs verwendet werden. Ein weiterer Aspekt betrifft die Vergleichbarkeit von Testergebnissen aus verschiedenen Testplattformen, um eine Gesamtargumentation zu ermöglichen. Die verschiedenen verfügbaren Testplattformen müssen für die Argumentation komplementär genutzt werden. Die Testorchestrierung sorgt für eine optimierte Nutzung der Plattformen basierend auf den relevanten Inputs:

- Testobjekte, Ziele und Szenarien
- Ziel-KPIs und Metriken
- Verfügbare Testplattform

Um eine optimale Nutzung zu gewährleisten, ist ein tiefes Wissen über die verfügbaren Testplattformen erforderlich. Dazu gehören verschiedene Eigenschaften und Verhaltensweisen der Testplattformen, um daraus Stärken und Schwächen abzuleiten. Ein Auszug der Eigenschaften ist in Abbildung 208 dargestellt.

Abbildung 208: Unterschiedliche Merkmale von Testplattformen

Um diese Eigenschaften zu analysieren, wird ein systematischer Vergleich von Testplattformen durchgeführt. Als Input für die Testorchestrierung soll sie eine individuelle Auswahl und Kombination innerhalb der Testorchestrierung ermöglichen. Je nach Grad der Integration in das Gesamtsystem können Testplattformen in reale, semi-reale und simulierte unterteilt werden. Bei virtuellen Testplattformen werden die fehlenden Teile des Gesamtsystems durch simulative Teile abgedeckt (z.B. Restbussimulation des fehlenden Fahrzeugbusses). Die Testplattform beschreibt den grundsätzlichen Aufbau bzw. Ansatz. Es ist zu beachten, dass nicht jede Funktionalität des Fahrzeugs auf jeder Testplattform getestet werden kann. Wird eine bestimmte Plattform angesprochen, wie z.B. der Hardware-in-the-Loop-Prüfstand für die Fahrassistenz, so wird diese spezifische Version als Testinstanz bezeichnet. Konkrete Szenarien können auf Testinstanzen ausgeführt werden.

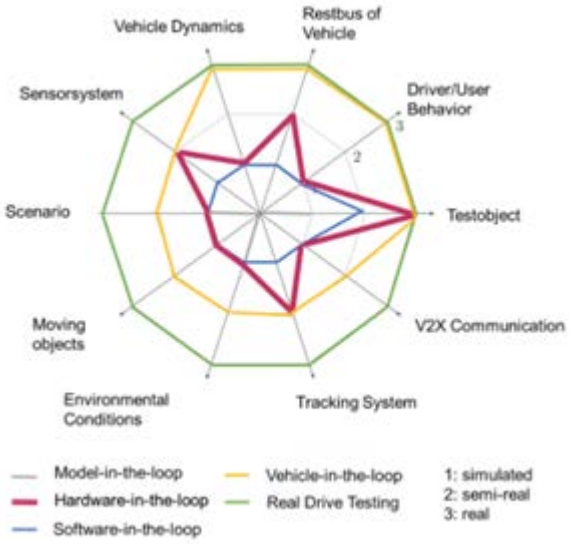


Abbildung 209: Vergleich verschiedener Testplattformen auf der Grundlage des Integrationsgrads.

Eine ausführliche Darstellung von Evaluationskriterien für Testinstanzen findet sich im öffentlichen Deliverable D12.

3.1.2.7.3 Exemplarische Realisierungen

Im nächsten Kapitel werden die entwickelten Ansätze des VVM in Bezug auf die Testmethodik vorgestellt.

Eine Übersicht ist in Abbildung 210 zu finden.

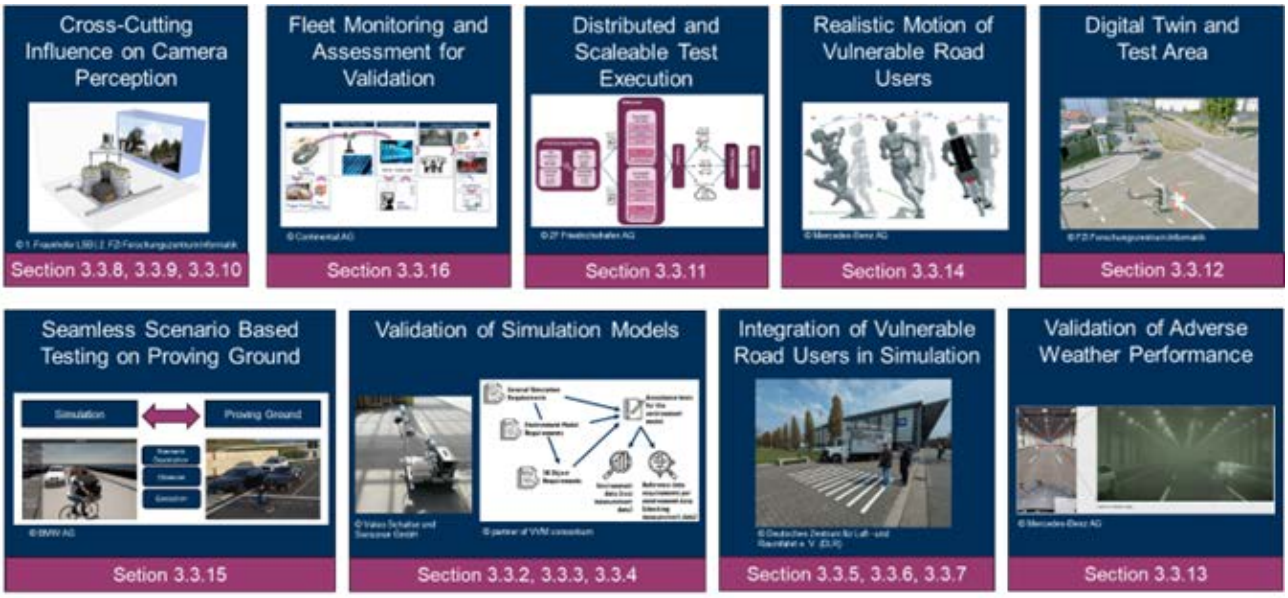


Abbildung 210: Überblick über die Testmethodik-Bausteine aus VVM.

3.1.2.7.3.1 Testmittelvalidierung, Sensormodellvalidierung, HIL-Demonstrator

Motivation

Um einen LiDAR-Sensor in Simulationsanwendungen einsetzen zu können, ist ein validiertes Modell des verwendeten Sensors erforderlich. Der Validierungsprozess ist daher wichtig, um realistische und vertrauenswürdige Simulationsergebnisse zu erzeugen. Dies geschieht durch den Vergleich von Daten aus der realen Welt mit Daten, die aus dem Sensormodell generiert wurden.

Aufbau und Funktionsweise

Auf dem Cobot-HiL-Prüfstand von Valeo wurden mit dem LiDAR "Scala Generation 1" Punktwolken von Asphalt im Abstand von 2 m und 10 m aus verschiedenen Winkeln aufgenommen. Die Messungen wurden auf dem firmeneigenen Werksgelände am Standort Kronach durchgeführt.

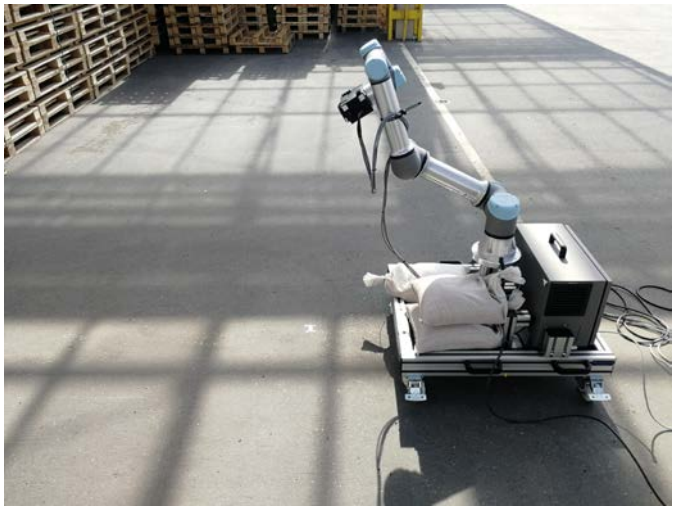


Abbildung 211: Cobot HiL im Betrieb (© Valeo Schalter und Sensoren GmbH)

Um die Abstände und Winkel zu realisieren, wurde der Sensor an einem Roboterarm montiert, was die erforderliche Sensorpositionierung und -ausrichtung ermöglichte (siehe Abbildung 211). Das Aufzeichnen der LiDAR-Punktwolke und die Bewegung des Roboterarms wurden von einem Laptop gesteuert. Ein Tachymeter diente zur Kalibrierung, zur Überprüfung der Sensorposition und -ausrichtung sowie zur Vermessung des Sensors in einem globalen Koordinatensystem. Wie in Abbildung 3 dargestellt ist, hat der LiDAR-Sensor ein horizontales Sichtfeld von 145° und ein vertikales Sichtfeld von 3,2°, unterteilt in 4 Schichten.

Technische Ausführung

Für zwei Messreihen "2 m" und "10 m" wurden jeweils neun Sensorpositionen und -ausrichtungen berechnet, so dass der Abstand vom Sensor zum Boden genau 2 m bzw. 10 m betrug und der Sensor auf den Messpunkt am Boden ausgerichtet war. Somit ergab sich für die Positionen eine Kreisbahn um den Messpunkt am Boden. Aufgrund des begrenzten Bewegungsumfangs lagen die Sensorpositionen in einem kurzen Segment dieser Kreisbahn. Dies ist in Abbildung 2 dargestellt.

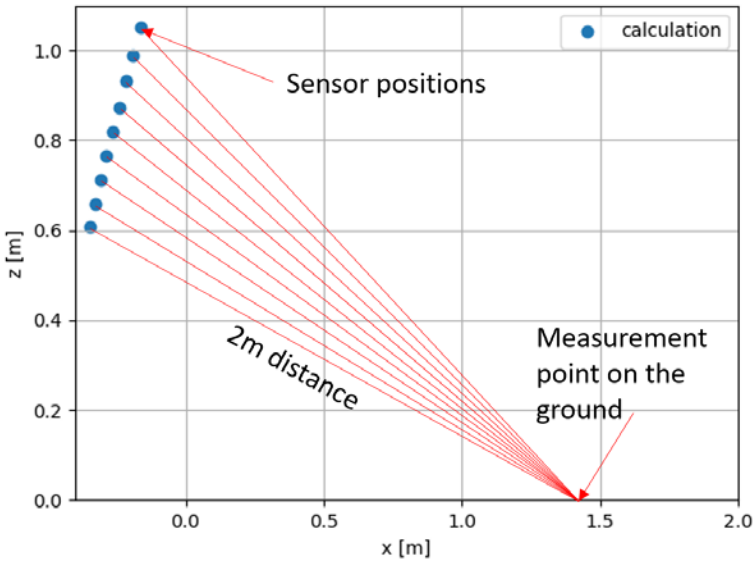


Abbildung 212: Sensorpositionen für Messungen in 2 m Entfernung (© Valeo Schalter und Sensoren GmbH)

Ein Beispiel für eine LiDAR-Messung für die Entfernung von 2 m ist in Abbildung 213 dargestellt.

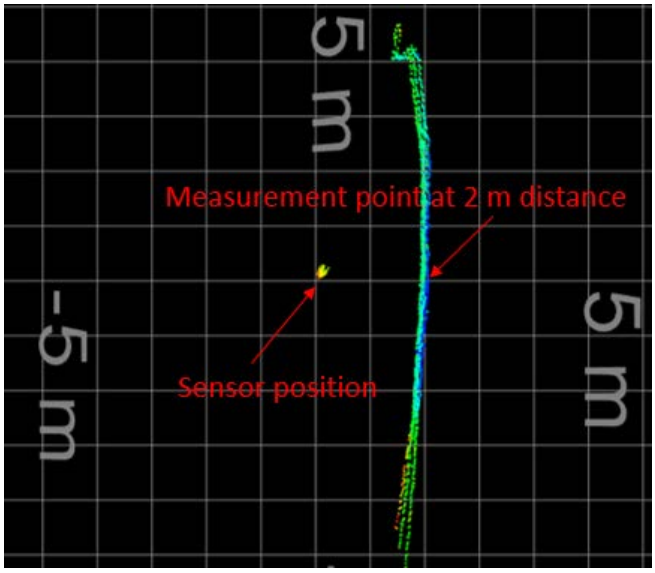


Abbildung 213: Visualisierung von Punktwolkendaten für eine Messung in 2 m Entfernung (© Valeo Schalter und Sensoren GmbH)

Einbindung in das VVM-Konzept

Das physikalische Testobjekt des Cobot HiL ist der "Scala Generation 1" LiDAR, dessen physikalische Zielgrößen Echopulsweiten und Punktwolken sind. Die von der HiL-Plattform gewonnenen Messdaten wurden zur Validierung eines Sensormodells verwendet. Das Hauptziel dieses Modells besteht auf technischer Ebene darin, ausgewählte Eigenschaften, insbesondere die Reflexionseigenschaften der realen Welt, widerzuspiegeln. Validierte Modelle, wie auch das Sensormodell, werden in der Testorchestrierung verwendet, um verschiedene Szenarien in Simulationen zu testen. Der Cobot HiL ermöglicht eine Bewertung der Vertrauenswürdigkeit des LiDAR-Modells und trägt damit wesentlich zur Validität und Aussagekraft des Sensormodells bei.

Testmittelvalidierung, Umgebungsmodellvalidierung**Motivation**

Eines der Hauptziele von VVM ist es, die Simulation als valides Werkzeug zum Testen automatisierter Fahrsysteme einzusetzen. Um zu beweisen, dass die Simulation ein valides Werkzeug ist, sollten alle verwendeten Simulationsmodelle validiert werden. Dieser Abschnitt zeigt, wie ein Umgebungsmodell validiert werden kann.

Anforderungen an ein validiertes Umgebungsmodell

Die folgende Abbildung zeigt ein Verfahren, wie ein Umgebungsmodell validiert werden kann. Das Verfahren ist in 3 verschiedene Abstraktionsebenen von Anforderungen gegliedert, wie die folgende Abbildung 214 dargestellt.

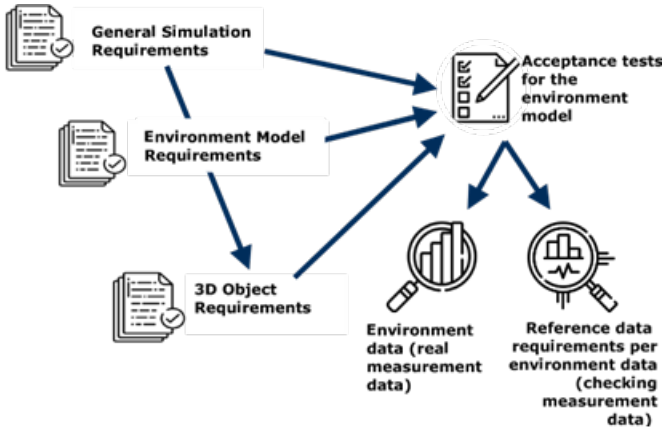


Abbildung 214: Validierungsverfahren

1. Allgemeine Simulationsanforderungen

Allgemeine Simulationsanforderungen umfassen verschiedene Aspekte wie Eingabedaten, Simulationsmodelle, Simulationsergebnisse, Dokumentation und andere relevante Faktoren, die zur erfolgreichen Ausführung und sinnvollen Interpretation von Simulationsanwendungsfällen beitragen. Allgemeine Simulationsanforderungen werden aus Expertenwissen, Unfalldaten, ODD, relevanten Normen und Vorschriften abgeleitet. Die folgende Tabelle zeigt ein Beispiel für allgemeine Simulationsanforderungen:

Tabelle 6: Beispiele für Simulationsanforderungen

ID	Beschreibung	Typ
Sim_Anf_1_1	Ein (globales) Koordinatensystem muss eindeutig definiert sein.	Allgemeine Anforderungen an die Simulation
Sim_Anf_1_2	Das Simulationswerkzeug muss OpenDRIVE in Version 1.6 unterstützen.	Allgemeine Anforderungen an die Simulation
Sim_Anf_1_3	Das Simulationswerkzeug soll Log-Dateien erzeugen.	Allgemeine Anforderungen an die Simulation

2. Anforderungen an das Umgebungsmodell

Die Anforderungen an das Umgebungsmodell müssen den beabsichtigten Zweck, den Detaillierungsgrad sowie die für das zu validierende System relevanten Aspekte berücksichtigen:

- physikalische Gesetze.
- Eigenschaften und Wetterbedingungen, die das Sensorverhalten beeinflussen können.
- Verkehrsregeln und Verhalten der Verkehrsteilnehmer.

Die Anforderungen an das Umgebungsmodell werden in Abhängigkeit von den allgemeinen Anforderungen, der geplanten Systemarchitektur und den Systemkomponenten abgeleitet. Die folgende Tabelle zeigt ein Beispiel für Umgebungsmodellanforderungen:

Tabelle 7: Beispiel für Umgebungsmodellanforderungen

ID	Beschreibung	Typ
Sim_Anf_2_1	Das europäische Straßenschild "Zebrastreifen" muss im Umgebungsmodell vorhanden sein und realistisch dargestellt werden können.	Umgebungsmodell-Anforderung

3. Anforderungen an 3D-Objekte

Die Anforderungen an die 3D-Objekte stellen sicher, dass die Oberflächeneigenschaften, die logischen Eigenschaften und der Detaillierungsgrad mit den Anforderungen des Sensors übereinstimmen:

- Wellenlängenbereich des Sensors.
- Ausgewähltes physikalisches Modell der Oberfläche von Objekten.
- Detaillierungsgrad des Objektnetzes.

Die Anforderungen an das 3D-Objektmodell ergeben sich aus den Umgebungsanforderungen, der geplanten Systemarchitektur und den Systemkomponenten. Die folgende Tabelle zeigt ein Beispiel für die Anforderungen an 3D-Objekte:

Tabelle 8: Beispiel für die Anforderungen an 3D-Objekte:

ID	Beschreibung	Typ
Sim_Anf_3_1	Der Wellenlängenbereich der BRDF muss den Wellenlängenbereich des Sensors umfassen.	3D-Objekt-Anforderungen

3.1.2.7.3.2 Testexecution; Simphera: Evaluation of an AD System Using Scenario-Based Testing

Motivation

Eines der Hauptziele von VVM ist es, die Simulation als valides Werkzeug zur Bewertung eines automatisierten Fahrsystems (AD) einzusetzen. Dazu ist es notwendig zu testen, ob das AD-System kritische Szenarien bewältigen kann. Ein kritisches Szenario zu finden, kann jedoch eine schwierige Aufgabe sein, da aus einem logischen Szenario mehrere konkrete Szenarien abgeleitet werden können. Eine Möglichkeit besteht darin, jedes konkrete Szenario parallel zu simulieren und zu testen, da jedes konkrete Szenario unabhängig von den anderen ist. Die Verwendung eines Computerclusters kann diese Aufgabe beschleunigen (szenariobasiertes Testen) und vermeidet den Aufwand, geeignete Parameter zu finden, die die Anzahl der konkreten Szenarien reduzieren.

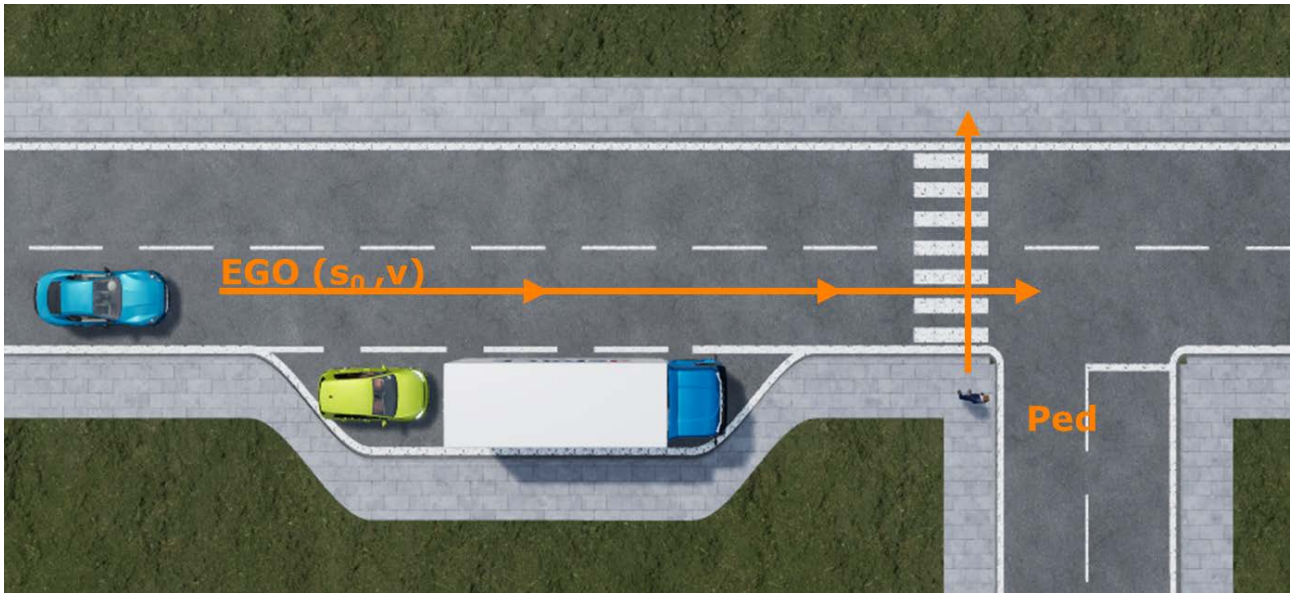


Abbildung 215: Beispiel für ein logisches Szenario: Ein Fahrzeug mit einem automatisierten Fahrsystem nähert sich einem Zebrastreifen. Ein Fußgänger, der von einem geparkten Auto verdeckt wird, möchte die Straße auf dem Zebrastreifen überqueren. Um das AD-System zu bewerten, muss eine Reihe von Parametern überprüft werden, um sicherzustellen, dass der Fußgänger nicht angefahren wird.

Tabelle 9: Parameter des Beispiels aus Abbildung 215

	Ego S_0 [m]	Ego v [km/h]	Ped S_0 [m]	Ped v [km/h]
Minimum	0	0	-20	0
Maximum	75	60	0	10
Schrittweite	5	5	1	1
Anzahl Parameter	15	12	20	10

Tabelle 9 zeigt die Parameter, die als Beispiel herangezogen werden. Ausgehend von den Parametern enthält der Parameterraum 32.000 konkrete Szenarien, mit denen das AD-System umgehen muss. In diesem Parameterraum gibt es bekannte und unbekannte Risiken. Durch das Testen des gesamten Parameterraums werden auch bekannte und unbekannte sichere Zustände ermittelt (siehe Abbildung 216).

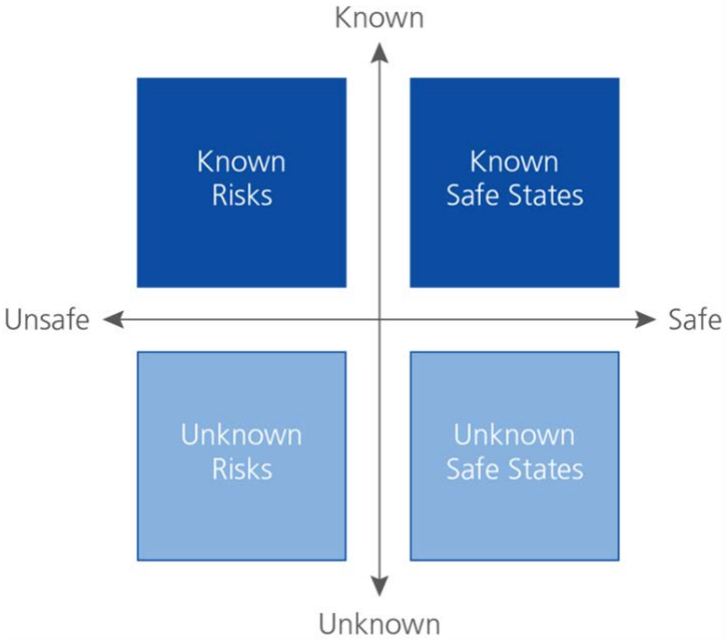


Abbildung 216: Parameterraums mit bekannten und unbekannten sicheren Zuständen.

Wenn das automatisierte Fahrsystem den Fußgänger in keinem Szenario trifft, kann das AD-System als sicher bewertet werden. Die Verwendung eines ISO 26262-zertifizierten Tools wie SIMPHERA kann diese Bewertungsaufgabe unterstützen.

3.1.2.7.3.3 Testorchestrierung, Simulationsvalidierung

Vergleich von Prüfstands- und Simulationsdaten eines SAE Level 4 Systems

Das Ziel dieser Aktivität war es, den Realitätsgrad einer detaillierten Simulation für ein automatisiertes Fahrzeug zu bewerten und eine Methode zur Bewertung der Gültigkeit der Simulationsergebnisse zu entwickeln und anzuwenden.

Abbildung 217: Linksabbiegeszenario mit fahrender SAE 4-Automatisierung (oben) im Testgelände, Realfahrt (unten) in der Simulation (© Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR))

Vorgehensweise

- Auf einem Testgelände werden ausgewählte Szenarien mit einem automatisierten Fahrzeug durchgeführt.
- Ein Modell des Fahrzeugs mit der gleichen Automatisierungsfunktion wird in die Simulation eingefügt.
- Das aufgezeichnete Verhalten der anderen Verkehrsteilnehmer auf dem Testgelände wird in der Simulation als Replay eingespielt.
- Das Simulationsergebnis wird mit den Referenzdaten verglichen.
- Unstimmigkeiten werden analysiert und ergründet, wobei zusätzlich zu den externen Verhaltensdaten auch interne Daten des Testfahrzeugs verwendet werden.

Versuchsaufbau

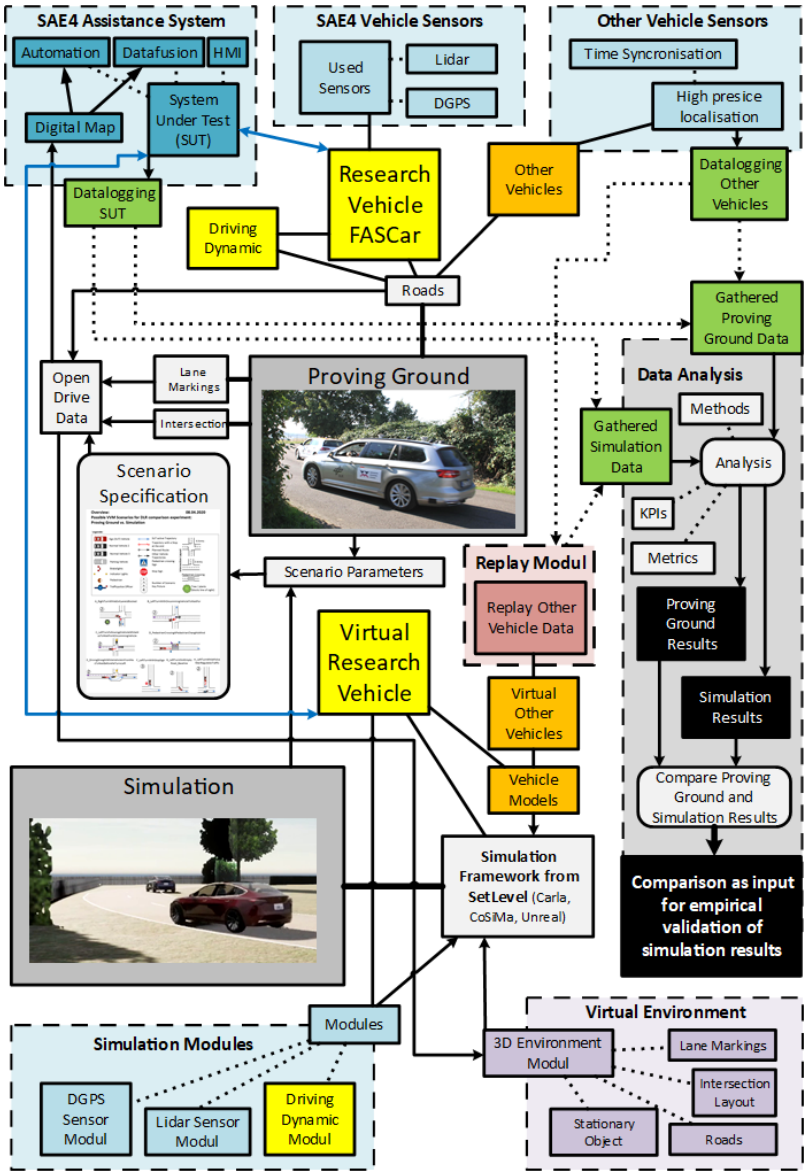


Abbildung 218: Komponenten und Abhängigkeiten des Versuchsaufbaus zum Vergleich und zur Auswertung gesammelter Prüfstands- und Simulationsdaten (© Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR))

Beispiel-Szenario

Das folgende Beispiel zeigt ein Linksabbiegeszenario, bei dem das automatisierte Fahrzeug den Gegenverkehr beachten muss.

Abbildung 219: Szenario - Linksabbiegen auf dem Testgelände, grüne Linie zeigt den Weg des automatisierten SAE 4 Fahrzeugs, rote Linie den Gegenverkehr (Daten © Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR), Luftbildkarte © Stadt Braunschweig, 2020)

Beobachtungen

- Die Diskrepanzen bei Position und Timing sind moderat.
- Artefakte bei der Wahrnehmung von Daten aus dem Testgelände.
- Physikalische, dynamische und Sensormodelle erfordern eine geeignete Kalibrierung.

Vergleich und Ergebnisse

- Simulationen können durch verschiedene Feinabstimmungen an die Realität angepasst werden.
- Abweichungen können dennoch beobachtet werden, wobei das Maß der maximal zulässigen Abweichung je nach Anwendung festgelegt werden muss.
- Erfassungsfehler (z.B. Geisterobjekte bei LiDAR) sind in den verwendeten Sensormodellen unterrepräsentiert.

Schlussfolgerungen

Die gewählte Werkzeugkette demonstriert die Fähigkeit der Simulation, die Realität genau abzubilden und SAE 4-Automatisierungssysteme zu validieren.

3.1.2.7.3.4 Testexecution; VRU-Integration in Simulationen

Simulationsmethoden wie Human-in-the-Loop oder Model-in-the-Loop wurden entwickelt und werden in immer mehr Anwendungsbereichen eingesetzt. Dies liegt vor allem daran, dass sie verschiedene Vorteile bieten, wie z. B. geringere Kosten oder ein geringeres Risiko. Im Automobilsektor werden diese Simulationsmethoden zur Simulation des Verkehrs, einschließlich ungeschützter Verkehrsteilnehmer ("Vulnerable Road User", VRU), eingesetzt. Die Modellierung des VRU-Verhaltens in der Simulation ist mit einigen Herausforderungen verbunden, z. B. aufgrund der hohen Freiheitsgrade und der spontanen Entscheidungsfindung des Menschen im Vergleich zu anderen Verkehrsteilnehmern. Ein generelles Ziel der Simulation ist es, die Realität so realistisch wie möglich abzubilden. Um eine realistische Simulation zu erreichen, müssen die

Komponenten und Akteure kalibriert werden. Für die Kalibrierung werden Daten aus der realen Welt benötigt, um die Simulationsdaten mit den Daten aus der realen Welt abzugleichen und in Übereinstimmung zu bringen. Diese Daten können mit verschiedenen Methoden gesammelt werden. In diesem Projekt wurden zwei Methoden verwendet, die im Folgenden kurz vorgestellt werden.

VRU Fußgänger-Simulator

Abbildung 220: MoSAIC Virtual Reality Fußgängersimulator VRU mit unbegrenzter Fortbewegung (© Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR))

MoSAIC (Modular and Scalable Application Platform for ITS Component) unterstützt die natürliche und uneingeschränkte 360°-Lokomotion innerhalb der Simulation auf einem Laufband mit 4,7 m Durchmesser. Ein am Kopf befestigtes Display ermöglicht es dem Benutzer, sich frei umzusehen ("360°"). Ganzkörper- und Gestenerfassung ermöglichen eine präzise Animation des Avatars des Benutzers. Dadurch kann der Benutzer direkt und indirekt mit anderen verbundenen Benutzern und Agenten über die simulierte Umgebung kommunizieren. Der VRU Fußgängersimulator kann mit anderen Simulatoren oder Systemen, wie z.B. einer ADAS/AD-Funktion, gekoppelt werden. Diese Simulationsstruktur ermöglicht eine hohe Präsenz des Benutzers in der Simulation und eine genaue Erfassung des Benutzerverhaltens.

VRU Augmented Reality Demonstrator

Abbildung 221: Augmented Reality VRU-Integration in einem Simulator (© Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR))

Diese VRU-Integration ist ein Objekterkennungssystem, das mit einem Verkehrssimulator und einem Augmented-Reality-Display gekoppelt ist. Die erkannten Objekte werden in der Simulation wiedergegeben und die simulierten Fahrzeuge interagieren mit den realen Objekten. Dieser Aufbau ist sehr flexibel und ermöglicht eine direkte Interaktion mit dem System ohne jegliche Vorbereitung des Benutzers.

Schlussfolgerung

Die Anwendung der vorgestellten Methoden zur Erfassung von VRU-Daten und zur Simulation von VRUs ermöglicht die Kalibrierung der Simulation, die Überprüfung der Gültigkeit von Szenarien, die Beobachtung kritischer Szenarien ohne Risiko und unterstützt schließlich die Absicherung des automatisierten Fahrens [107].

Abbildung 222: Beispielhafte Visualisierung eines Zebrastreifens innerhalb der VRU-Simulation (© Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR))

3.1.2.7.3.5 Szenario basiertes Testen auf Prüfgeländen

Hauptziele

- Automatisierte Durchführung von komplexen Testszenarien (z.B. Fahrdynamik, Dauertest) auf einem Testgelände zur Gewährleistung reproduzierbarer Ergebnisse in einer sicheren Umgebung.
- Nahtlose Interaktion von Prüfstandversuchen mit einer Simulation, um evidenzbasierte Ergebnisse zu gewährleisten.

Technische Ziele

- Verifizierung der Trajektorienplanung des Ego-Fahrzeugs für Simulation und reale Tests auf einem gemeinsamen, definierten Szenario-Beschreibungsstandard (ASAM OpenScenario 2.0).
- Entwicklung eines Kontrollzentrums als zentrale Einheit die alle automatisierten Testteilnehmer koordiniert (Fahrzeuge, bewegte Plattformen, etc.).
- Sicherheit, wie Geofencing-Überwachung des Testgeländes (kontrollierter klassischer / automatisierter Verkehr).

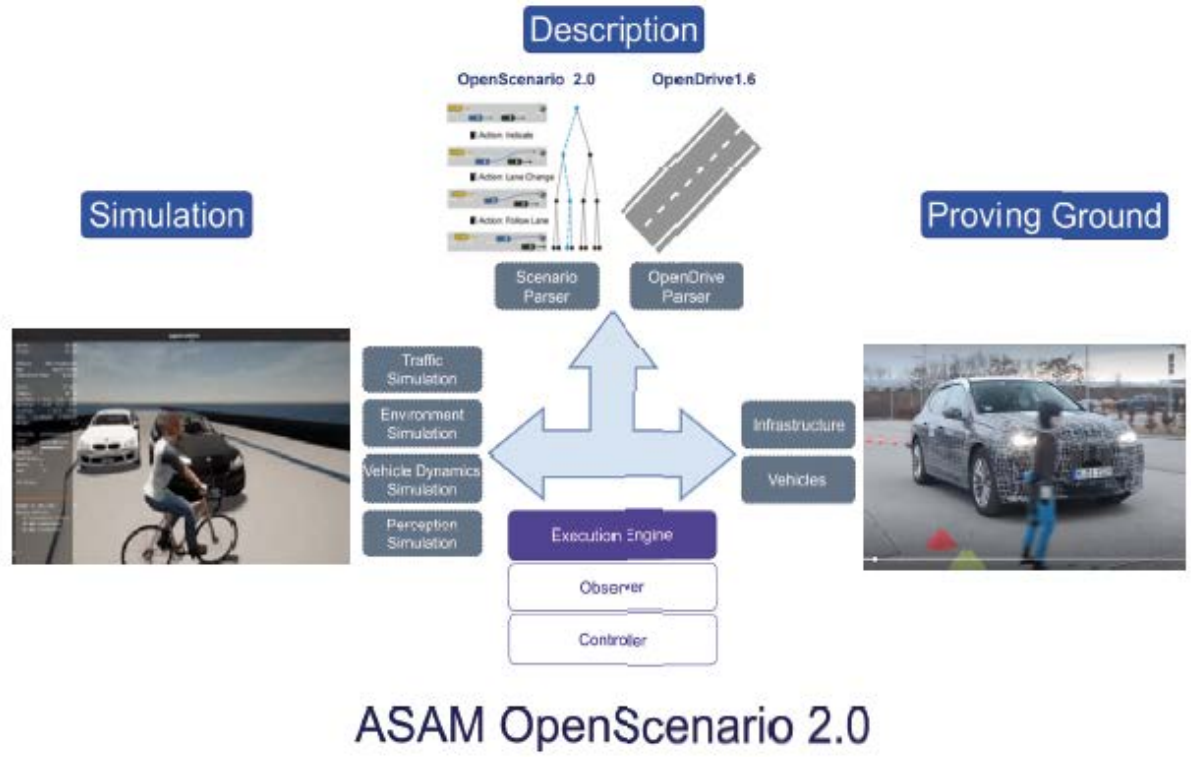


Abbildung 223: Open Scenario als gemeinsames Format zur Szenariobeschreibung in der Simulation und für reale Tests (© 1. BMW AG| 2. BMW AG)

Ansatz

- Implementierung für VVM-Verkehrsszenarien mit koordinierter Robotik inklusive Versuchsdurchführung und Demonstration des funktionalen Use-Case (FUC2.3).
- Szenariobeschreibung basierend auf der Definition des ASAM OpenScenario 2.0 und OpenDrive1.X Standard.
- Möglichkeit der Einbeziehung verschiedener Testplattformen mit unterschiedlichen Schnittstellen in ein Test-Set aufzunehmen.
- Reproduzierbare Steuerung von Verkehrsteilnehmern und dynamischer Straßeninfrastruktur.

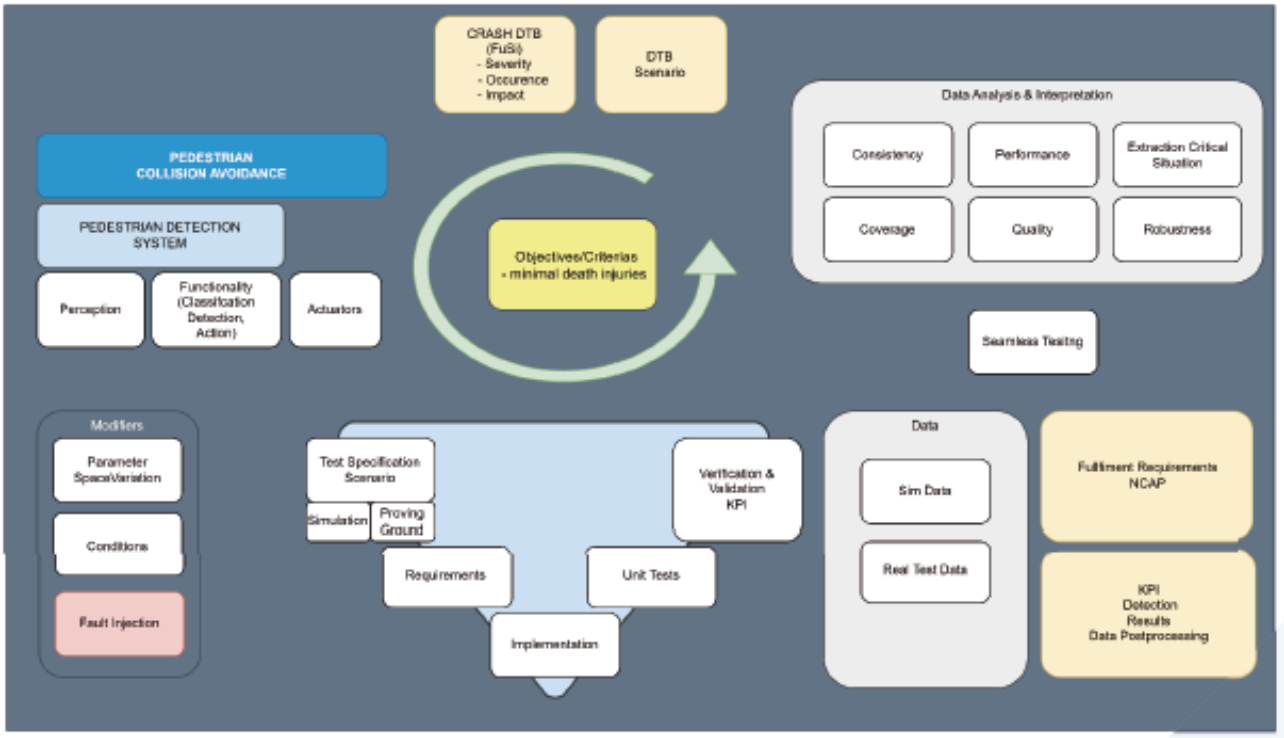


Abbildung 224: Einsatz- und Anwendungsbereiche für eine automatisierte Testumgebung / automatisiertes Testgelände (© 1. Akkodis Deutschland Consulting GmbH)

Umsetzung

- Fahrzeugsteuerung mit Einsatz von Robotik und/oder Steuergeräte-Manipulation. HMI-Interaktion mit Aktoren/Robotik (Simulation von Fahreraktivitäten).
- Entwicklung eines ROS2-Frameworks zur Steuerung eines automatisierten Multi-Teilnehmer-Test (Fahrzeuge, bewegliche Plattformen) über das Kontrollzentrum.

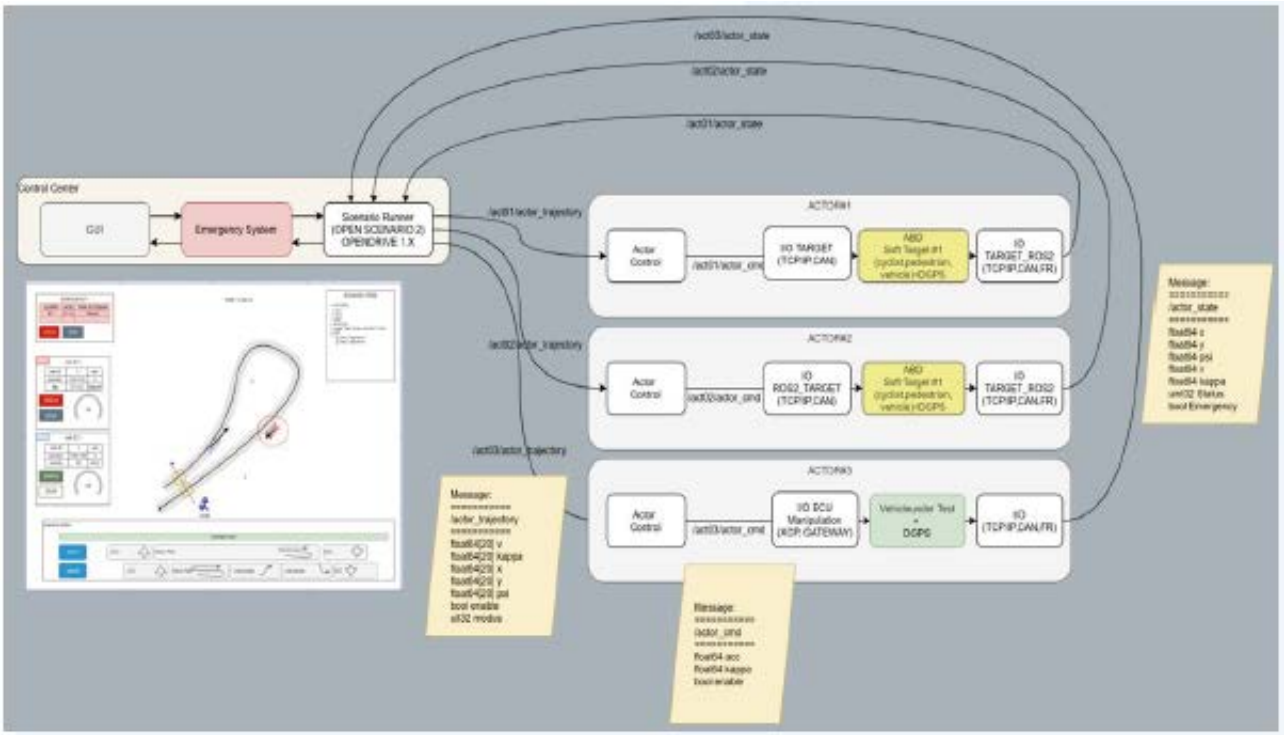


Abbildung 225: ROS2-Framework zur Integration vieler Testteilnehmer in ein Testszenario (Szenario © 1. Akkodis Deutschland Consulting GmbH)

Integration einer bewegten Plattform/Zielscheibe in das ROS2-Framework am Beispiel von 4activeSystems' Freeboard 4activeFB-small.

- ROS2-Schnittstelle.
- Trajektorienplanung der bewegten Plattform.
- Steuerung und Überwachung der beweglichen Plattform.
- Manuelle Fernsteuerung (vom Kontrollzentrum aus) mit Hilfe eines Joysticks.
- Trajektoriengenerierung (für alle Testteilnehmer) basierend auf der ASAM OSC2.0 Szenariobeschreibung.

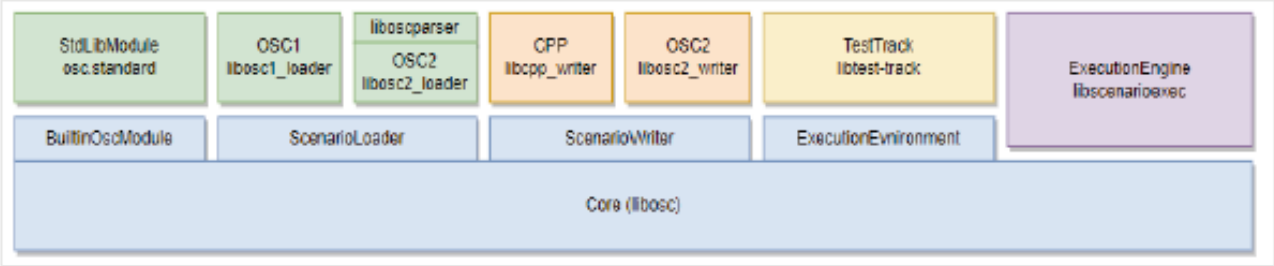


Abbildung 226: Entwicklungskomponenten für die Trajektorienextraktion auf Basis des ASAM OSC2.0 Standard (© 1. Akkodis Germany Consulting GmbH)

3.1.2.7.3.6 Schlechtwetterperformance von Sensoren - Validierung der Schlechtwetterleistung von automatischen Fahrsystemen (ADS)

Schlechtwetterperformance

Ähnlich wie beim Wahrnehmungssystem vom Menschen wird die Leistungsfähigkeit eines technischen Wahrnehmungssystems eines automatischen Fahrsystems (ADS) durch Schlechtwetter (Nebel, Regen, Gischt) degradiert. Zur Klärung der Fragestellung, bis zu welcher Degradationsstufe ein automatisches Fahrsystem seine Funktion sicher erfüllen kann, sind Messverfahren zur Evaluierung der Schlechtwetterperformance eines AFS notwendig. Diese wurden im Projekt VVM für die Schlechtwetterfälle Nebel, Regen und Gischt entwickelt. Während die Umgebungserfassungssensoren nur anhand von realem Schlechtwetter (simuliert in einer Schlechtwetter-Kammer bzw. einem Spray-Generator) geprüft werden können, ist eine Verifikation des nachgelagerten Wahrnehmungssystems des ADS hingegen wegen der Vielzahl der Testszenarien nur digital auf der Basis von simulierten Schlechtwettersensordaten möglich.

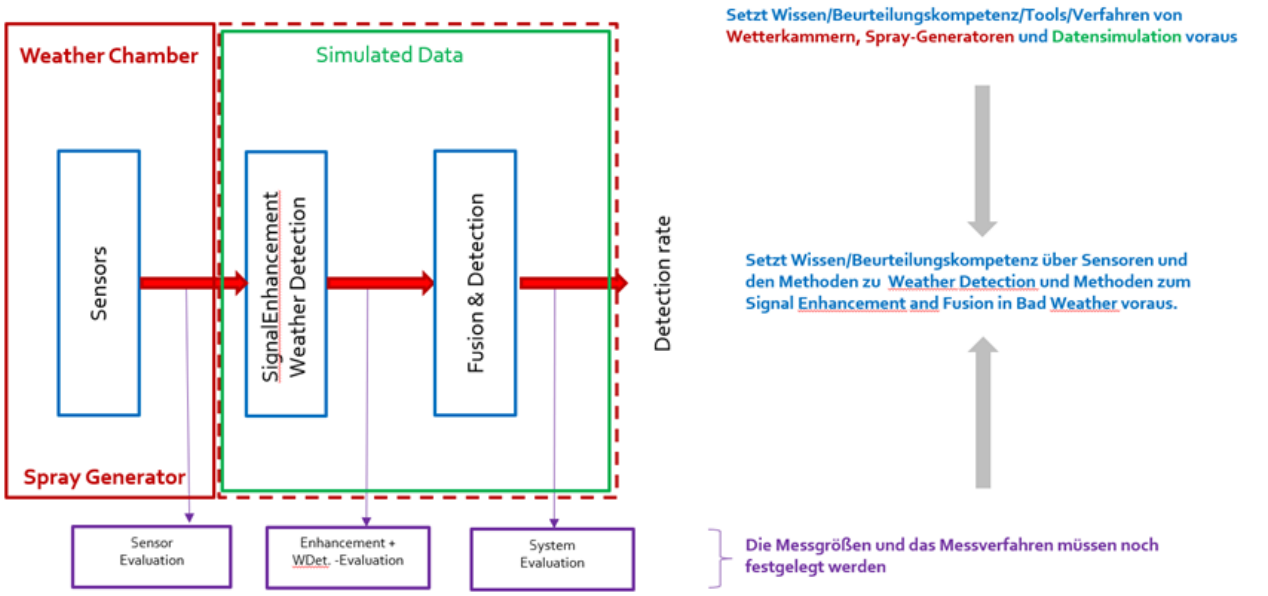


Abbildung 227: Schlechtwetterevaluationsschema für ADS. (© Mercedes-Benz AG)

Schlechtwetterperformance Gischt

Für die reale Simulation von Gischt haben wir zusammen mit der Fa. Messring einen portablen Gischtgenerator entwickelt, der mit geringem Aufwand in beliebige Testfahrzeuge verbaut werden kann (siehe Abbildung 228). Dieser erlaubt durch Wahl einer definierten Spraystärke und definierten Fahrmanövern (z.B. Vorausfahrt, Überholvorgang) den physikalischen Einfluss von Gischt auf ein Folgefahrzeug (Messfahrzeug) reproduzieren. Durch ebenfalls im Projekt entwickelten Messverfahren kann so wiederholbar der Einfluss von Gischt auf die Leistungsfähigkeit eines Sensors bzw. AFS, durch Wahl einer definierten Spraystärke und definierten Fahrmanövern (z.B. Vorausfahrt, Überholvorgang), zu bestimmen.

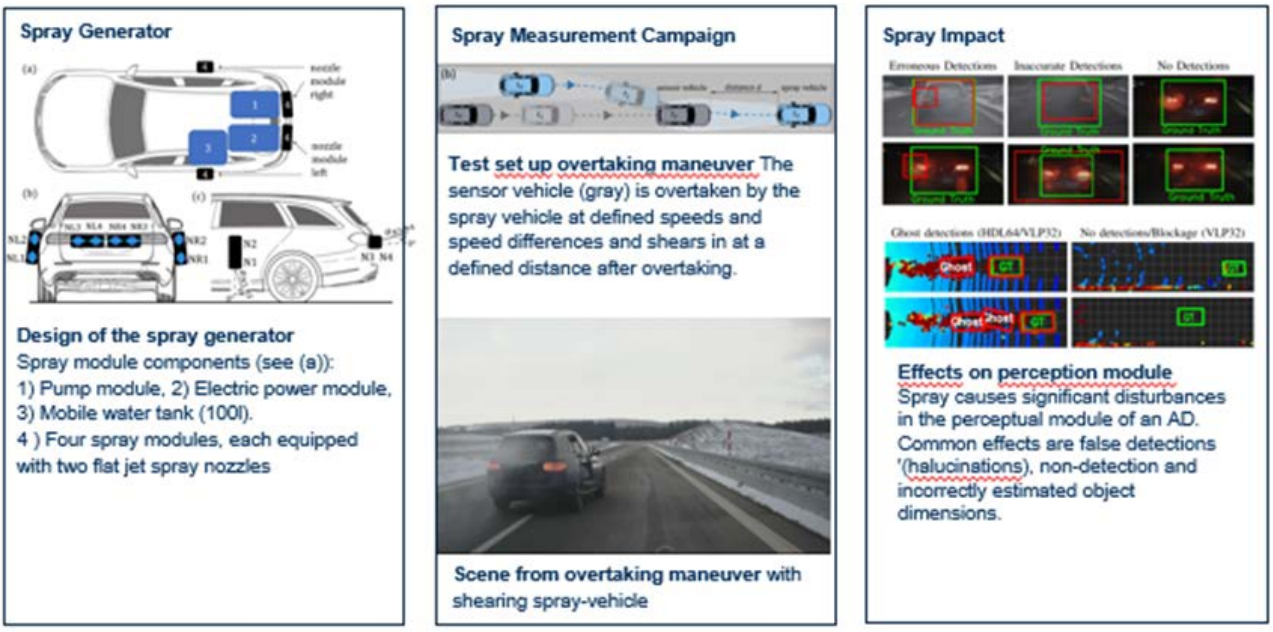


Abbildung 228: Gischtgenerator, Definition des Fahrmanövers „Überholen“ und die Auswertedaten aus diesem Test. (© Mercedes-Benz AG)

Sensor-Schlechtwetterperformance-Messungen basierend auf Wetterkammer-Daten

Der Einfluss von Nebel und Regen auf die Leistungsfähigkeit der Umgebungserfassungs-Sensoren von AFS lässt sich wiederholbar nur in Wetterkammern bestimmen. Nur hier kann der Schlechtwettergrad über die gesamte Messstrecke definiert eingestellt und gehalten werden. Die Bestimmung des Schlechtwettereinflusses erfolgt dabei auf der Basis der von uns definierten Messszenarien und den von uns entwickelten Evaluierungs-Metriken. Beispielhaft wird in Abbildung 229 ein Wetterkammerszenario für den Lost-Cargo-Fall gezeigt.

Abbildung 229: Wetterkammerszenario zum lost-cargo-test und ein Bildausschnitt daraus bei Nebel mit 80m Sichtweite. (© Mercedes-Benz AG)

AFS-Schlechtwetterperformance-Messungen basierend auf Simulationsdaten

Die Bestimmung der Schlechtwettertauglichkeit eines AFS setzt voraus, dies umfassend für alle Schlechtwettergrade, allen Eckpunktszenarios mit allen zu testenden Fahrmanövern durchzuführen. Für all diese Fälle Realweltsensordaten zu beschaffen, ist nicht machbar. Aus diesem Grund kann die Bestimmung der Schlechtwetter-Performanz eines AFS nur über Simulationsdaten erfolgen. Im Projekt haben wir eine Vielzahl von State of the Art Schlechtwetter-Sensordatensimulationen für Kamera und LiDAR entwickelt, auf deren Basis eine Bewertung der Schlechtwettertauglichkeit von AFS durchgeführt werden kann. Exemplarisch wird in Abbildung 230 das Ergebnis einer auf NeRF-basierten (Neural Radiance Fields-basierten) Nebelsimulation für Kamerabilder dargestellt.

Abbildung 230: Kamerabilder mit über NeRFs generierter unterschiedlich starker Vernebelung (links leichter Nebel, rechts starker Nebel) (© Mercedes-Benz AG)

3.1.2.7.3.7 Analyse und realistische Nachbildung ganzheitlicher Bewegungsmuster gefährdeter Verkehrsteilnehmer (VRU)

Zunehmender Bedarf an Tests unter realen Bedingungen

Mit dem klaren Ziel höhere Automatisierungsgrade und schließlich autonomes Fahren zu ermöglichen, macht die Entwicklung von Fahrerassistenzsystemen rasante Fortschritte. Ein Schwerpunkt der Entwicklung liegt auf der Verbesserung der Erkennung von ungeschützten Verkehrsteilnehmern (VRU) und der frühzeitigen Erkennung der Absichten von Personen anhand kleinster Bewegungen. Bisherige Systemtests beschränkten sich jedoch auf "statische" VRU-Dummys mit rein zweidimensionalen translatorischen Freiheitsgraden. Um diese Lücke zu schließen, wurde der folgende Ansatz gewählt:

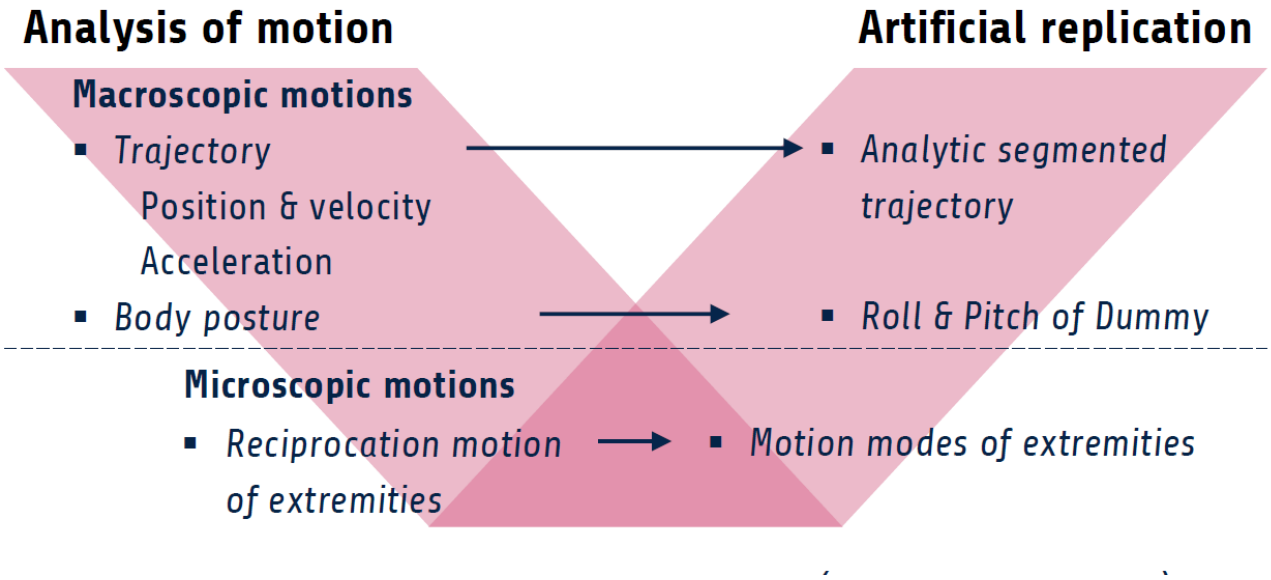


Abbildung 231: Abstraktionsmodell der Bewegungsmuster (© Mercedes-Benz AG)

Messung makroskopischer Bewegungen von Fußgängern und Radfahrern

Um eine Datenbasis zu schaffen, wurde eine Probandenstudie durchgeführt. Fußgänger und Radfahrer wurden hierfür mit Messsystemen ausgestattet, welches aus einem rtk-GNSS-System und einer Inertialmesseinheit (IMU) bestanden. Unterschiedliche Parameter der Körperhaltung und Bewegungstrajektorie der Probanden wurden untersucht:

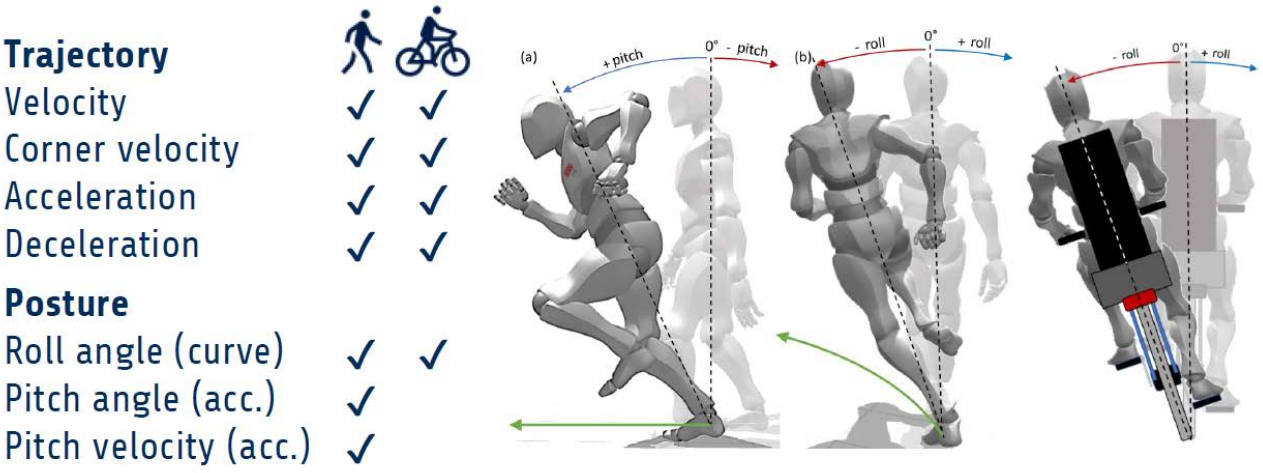


Abbildung 232: Untersuchte makroskopische Rotationswerte für Fußgänger und Radfahrer. (© Mercedes-Benz AG | MESSRING Active Safety GmbH)**Analyse und künstliche Nachbildung ausgewählter makroskopischer Bewegungsmuster**

Typische Geschwindigkeiten für unterschiedliche Gangarten sind in wissenschaftlicher Literatur einsehbar. Informationen zur Verteilung von Nick- und Rollwinkel sowie deren zeitlicher Verlauf sind weitestgehend unbekannt und waren deshalb Fokus der Untersuchung.

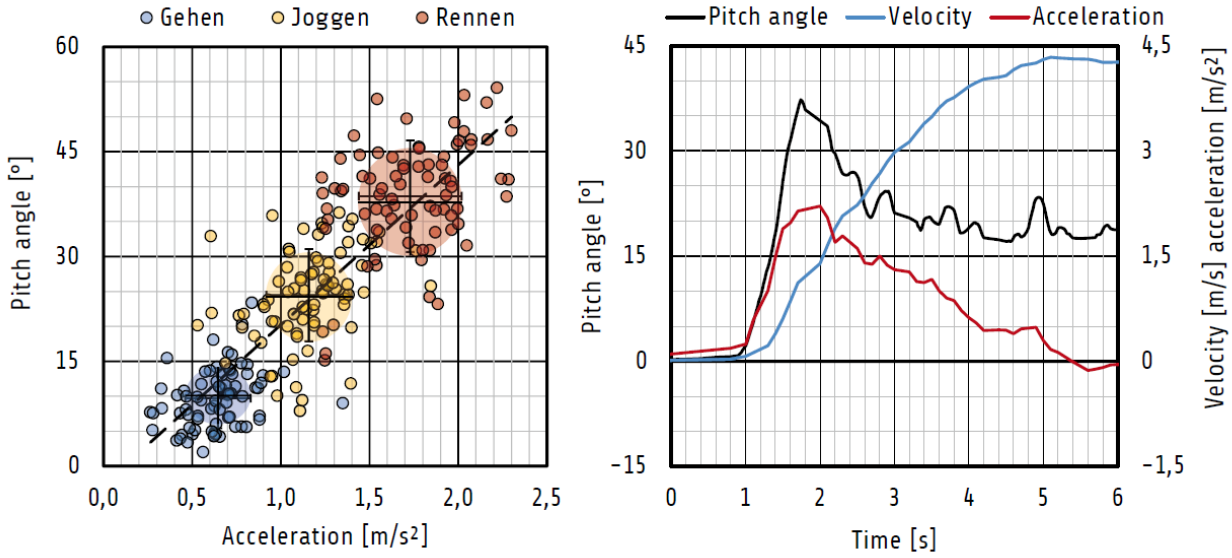


Abbildung 233: Verteilung der Maximalwerte des Nickwinkels während der Beschleunigung für verschiedene Gangarten (links) und Verlauf von Nickwinkel, Geschwindigkeit und Beschleunigung während der Startphase (© Mercedes-Benz AG | MESSRING Active Safety GmbH)

Die maximalen Nickwinkel während der Startphase zeigen eine deutliche Korrelation bezüglich der Beschleunigung. Dieser Zusammenhang wird analytisch beschrieben und entsprechend im prototypischen Prüfsystem implementiert. Im zeitlichen Verlauf (siehe Abbildung 233, rechts) zeigt sich, dass die Maximalwerte des Nickwinkels und der Beschleunigung zeitlich übereinstimmen. Nach dem initialen Maximum geht die Beschleunigung gegen null. Der Nickwinkel zeigt hingegen auch bei konstanter Geschwindigkeit einen deutlich positiven Wert, was eine Körperneigung nach vorne beschreibt.

Messung mikroskopischer Bewegungen

Die Bewegungen der Extremitäten wurden mit einem Motion-Capture-System, bestehend aus zehn IMU-Sensoren, erfasst. Die Anordnung der Sensoren und die abgeleiteten mikroskopischen Bewegungsparameter sind in Abbildung 234 dargestellt.

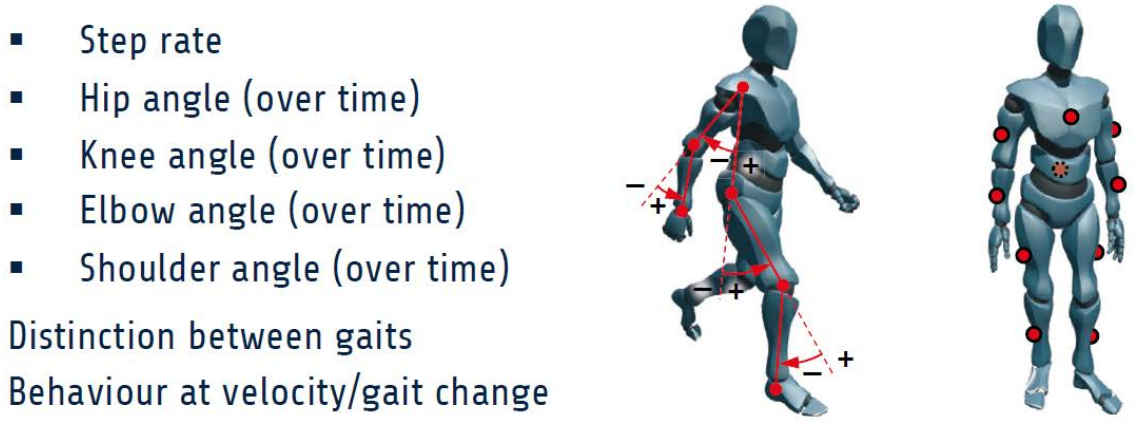


Abbildung 234: Untersuchte mikroskopische Bewegungswerte (links) und Platzierung der Motion Capture Sensoren. (© Mercedes-Benz AG | MESSRING Active Safety GmbH)

Analyse und künstliche Nachbildung ausgewählter mikroskopischer Bewegungsmuster

Wie in Abbildung 235 dargestellt, unterscheiden sich die Knie- und Hüftwinkel zwischen Probanden und dem Standard-NCAP-Dummy. Insbesondere bei hohen Geschwindigkeiten ist die Aktorik der Dummygelenke nicht in der Lage, genügend Kraft aufzubringen, um die Winkel präzise zu nachzubilden. Da das Kniegelenk nicht aktiv gesteuert wird, treten hier die größten Abweichungen auf. Eine deutliche Verbesserung kann durch den Einsatz fortschrittlicher Ansteuerungsmethoden erreicht werden, wie sie für den Advanced Motion Dummy (Astero) dargestellt sind.

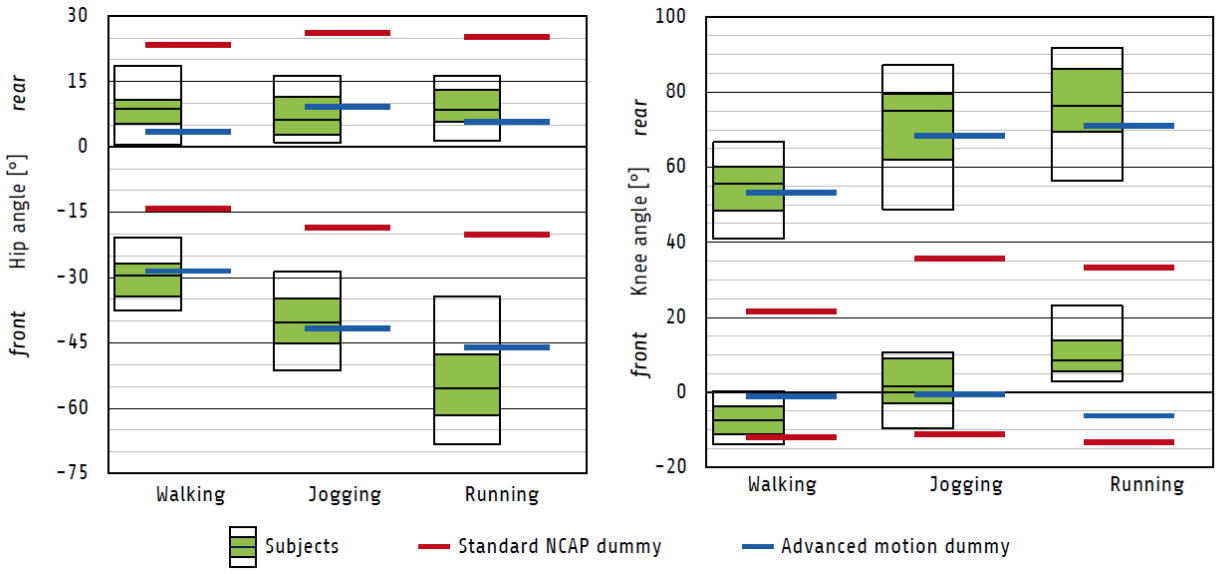


Abbildung 235: Vergleich der vorderen und hinteren maximalen Hüft- und Kniewinkel von Probanden , Standard-NCAP-Dummy und Advanced Motion Dummy bei verschiedenen Gangarten (© Mercedes-Benz AG | MESSRING Active Safety GmbH)

Schlussfolgerung

Mit dem entwickelten Verfahren wurde eine prototypische Umsetzung realisiert (Abbildung 236), welche ein realistischeres Bewegungsverhalten für VRUs ermöglicht. Damit ist Mercedes-Benz in der Lage, die Intentionserkennung zukünftiger Fahrerassistenzsysteme anhand marginaler Indikatoren wie der Schwerpunktverlagerung oder der Hüft- und Kniewinkel reproduzierbar zu testen und zu validieren. Dies ermöglicht neue Strategien in der Auslegung der Assistenten, die zu mehr Sicherheit im realen Leben beitragen.

Abbildung 236: Prototypische Realisierung des erweiterten Positionierungssystems und Dummy auf dem Mercedes-Benz Prüfgelände in Immendingen (© Mercedes-Benz AG)

3.1.2.7.3.8 Analyse von Umgebungseinflüssen unter Laborbedingungen

Ansatz

Im aktuellen Zustand können Umwelteinflüsse auf einzelne Komponenten der hochautomatisierten Wirkungskette nur auf einem sehr hohen Reifegrad getestet werden. Mit vollständiger Hardwareintegration werden Verifizierungen in realen Fahrtests durchgeführt, um eventuelle umgebungsbedingte Einschränkungen zu ermitteln. Dies bedeutet, dass Optimierungen von Designentscheidungen nicht während des laufenden Entwicklungsprozesses umgesetzt werden können. Darüber hinaus steigt das Risiko von Unfällen während eines realen Tests aufgrund eines unerwarteten Leistungsdefizits. Mittels unseres xiL-Demonstrators möchten wir eine frühzeitige Erkennung von Abhängigkeiten zwischen dekomponierten Zuständen und Umweltphänomenen in Bezug auf die Leistung der Hardware zeigen.

Dabei möchten wir Lösungsansätze aufzeigen:

- Testen der Kamerahardware mithilfe einer Kamerabox.
- Beaufschlagung der Kamera mit Vibrationsbelastungen mittels Mehrachskinematik.
- Die prozedurale Variation der Umgebung auf allen Straßenschichten.

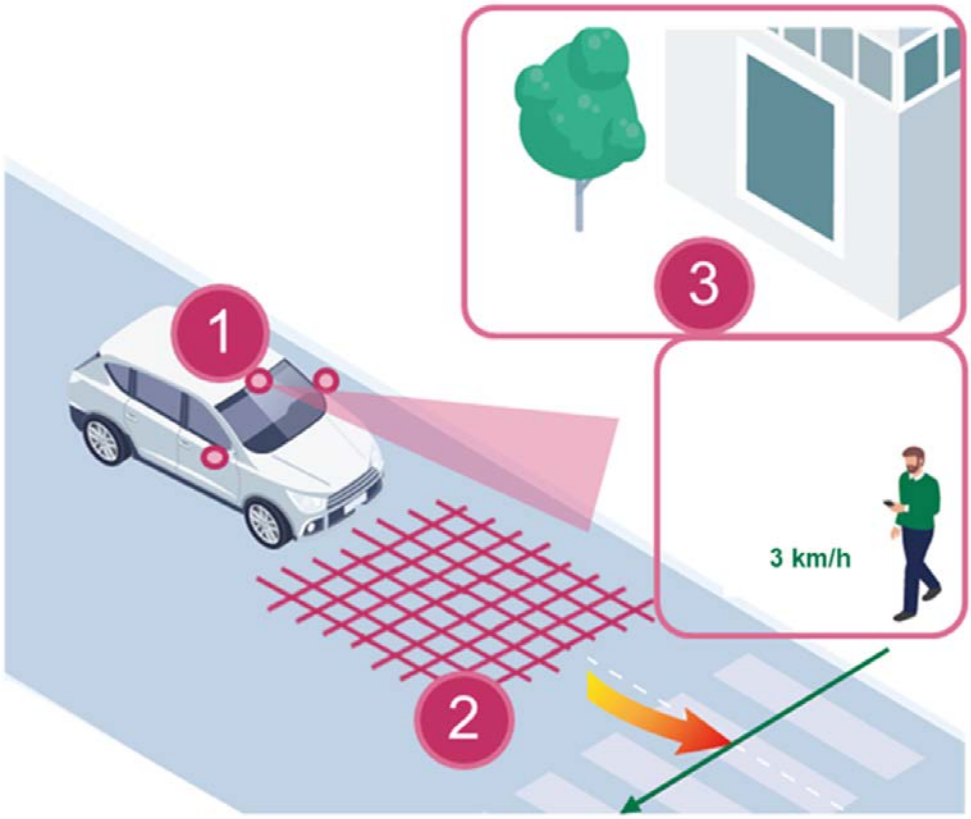


Abbildung 237: Abgezielte Realfahrten-Konditionen die unter Labor-Bedingungen verlagert werden sollen (© FZI Forschungszentrum Informatik)

Auswirkungen auf das Projekt

Als Aufgabe zur Realisierung einer exemplarischen Umsetzung einer Testinstanz im Szenario-basierten Testen wird der Vibrationsprüfstand als Hardware-in-the-Loop-Testplattform für die

Ursache-Wirkungsketten spezifiziert. Der Prüfstand liefert Informationen über die kinematische Kopplung zu einem konkreten Wahrnehmungsmodus (Kamera) durch eine systematische Analyse. Die Eingabe erfolgt durch Vorgabe eines Szenarios in einer virtuellen Fahrzeugsimulation, die die Beschleunigung des Kameraanbindungspunktes für Geschwindigkeiten zwischen 10 und 30 km/h auf einem Straßenprofil (Kopfsteinpflaster mit 25 cm breiten Steinen; z.B. als OpenCRG-Datei).

Der Prüfstand ermöglicht die Variation der gesamten kinematischen Fahrzeugeigenschaften im Frequenzbereich bis etwa 200 Hz, der vom Fahrzeug zur Kamera gekoppelt ist. Es ist möglich, durch das Erfassen des Leistungsdichtespektrums der Beschleunigungen am Kameraanbindungspunkt zunächst unabhängig von den restlichen Umgebungen lokale Leistungsminima durch das Frequenzspektrum zu bestimmen. Durch eine frühzeitige systematische Erfassung einer generischen Aussage, nämlich Leistungsverschlechterung in Abhängigkeit vom Frequenzspektrum, kann der Prüfraum erheblich reduziert werden. Unser Beobachtungsziel ist die Genauigkeit und Robustheit des bildbasierten Objektdetektors unter Test. Zusätzlich kann die visuelle Umgebung durch prozedurale Generierung variiert werden, um die Umgebung als Einflussfaktor auszuschließen und somit eine Kreuzvalidierung für die Frequenzaussage oder das Auffinden auslösender Objekte zu ermöglichen.

Abbildung 238: Abgezielte Realfahrten-Konditionen die unter Labor-Bedingungen verlagert werden sollen (© 1. FZI Forschungszentrum Informatik, 2. Fraunhofer LBF)

3.1.2.7.3.9 Testexcution; Analyse einer Wirkkette eines Wahrnehmungs-Testobjektes mit einer Hardware-in-the-Loop-Testplattform

Motivation

Rein softwarebasierte Simulationen können nicht alle hardware- und komponentenverbundenen Einschränkungen testen oder erfassen. Gleichzeitig sind Testläufe in der realen Welt mit allen relevanten Bedingungen (Verkehrsstruktur, Hindernisse, Wetter usw.) äußerst zeitaufwändig und führen nur zu schwer reproduzierbaren Variationen. Aus diesem Grund wird auch in Zukunft ein Prüfstand mit Hardware-in-the-Loop-Integration für die Bewertung von Fahrerassistenzsystemen (FAS) unverzichtbar sein. Dies unterstreicht die Notwendigkeit, Simulation und die reale Welt auf Prüfständen in Einklang zu bringen, um ihre jeweiligen Stärken und Schwächen besser zu verstehen.

Ein Simulationsmodell kann nicht alle Hardware-Einschränkungen repräsentieren. Ein Hardware-in-the-Loop-Prüfstand eignet sich besonders für:

- Begrenzung der Rechenleistung
- Rolling Shutter-Effekte der Kamera
- Zeitsynchronizität
- Einfluss von Störvariablen wie Temperatur und Vibrationen auf die Hardware

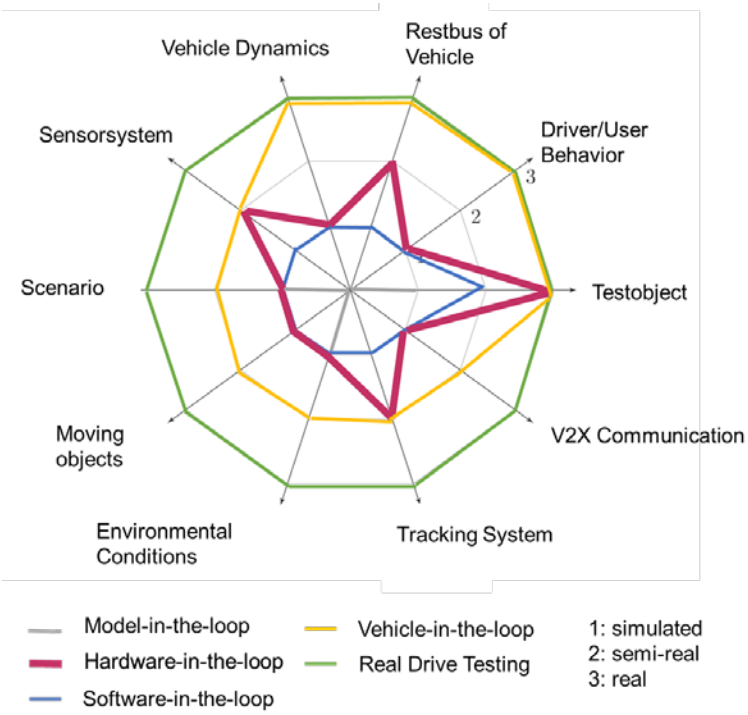


Abbildung 239: Affinitäten der Testtechnologien in den einzelnen Aspekten des Testen der hochautomatisierten Fahrfunktion (© 1. FZI Forschungszentrum Informatik)

Implementierung

Im Rahmen des VV-Methods-Projekts wurde am FZI ein Hardware-in-the-Loop (HiL)-Prüfstand entwickelt. Die wissenschaftliche und integrative Arbeit rund um den Prüfstand bewertet und ermöglicht die Automatisierung von Testprozessen, um wiederholbare und präzise Tests sicherzustellen. Er ermöglicht die koordinierte Durchführung verschiedener Testsszenarien und Sequenzen, um sicherzustellen, dass alle relevanten Aspekte des zu prüfenden Systems gründlich überprüft werden. Der HIL-Prüfstand ermöglicht die Erstellung und Anpassung von Testsszenarien zur Simulation unterschiedlicher Betriebsbedingungen und Umweltfaktoren. Tests können automatisch in SiL und HiL gestartet und überwacht werden, um die Effizienz der Testausführung zu steigern. Der HiL-Prüfstand erfasst und analysiert Messdaten, um die Leistung und Zuverlässigkeit des zu prüfenden Systems zu bestimmen. Das entwickelte Testobjekt umfasst die Automotive-Kamera Leopard Imaging IMX-490 mit der entsprechenden Recheneinheit der Nvidia Jetson Embedded Hardware. Softwareseitig mit unserer eigens entwickelten Late Fusion Architecture aus einer LiDAR und Bild-Objektdetektion/Klassifikation mit Positionsschätzung aus jeweils vortrainierten neuronalen Faltungsnetze aus der Open MMLab-Modellbibliothek und API eingebettet in einer ROS (Robot Operating System)-Umgebung.

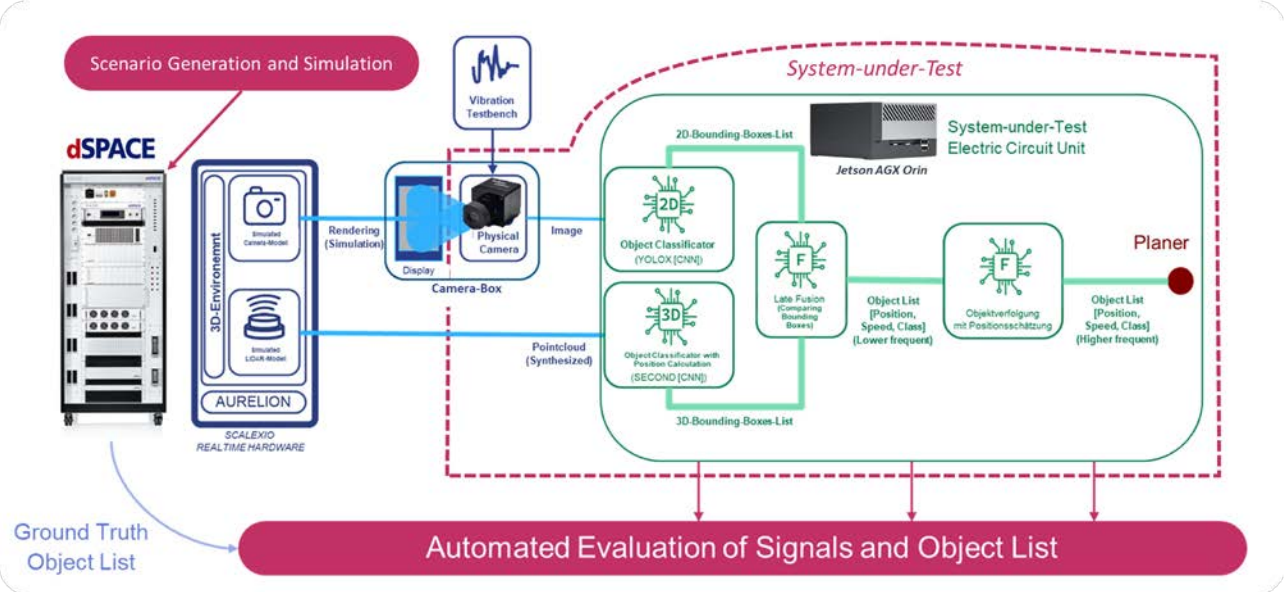


Abbildung 240: Wirkkette der integrierten Testplattform und des entwickelten Wahrnehmungstestobjektes (© 1. FZI Forschungszentrum Informatik)

3.1.2.7.3.10 Ein virtueller Prüfstand für die Entwicklung von hochautomatisierten Fahrfunktionen

Einleitung und Problemstellung

Die Erhöhung der bereits softwarebasierten Automatisierung von Fahrfunktionen hin zur vollständigen Autonomie ist ein angestrebtes Ziel für die absehbare Zukunft der globalen Mobilität. Zu diesem Zweck ist die nahtlose Integration zahlloser Software- und Hardwarekomponenten, aus denen sich diese cyber-physischen Systeme zusammensetzen, unabdingbar. Dazu gehört auch die Aggregation potenziell korrelierter Funktionen für die Fahrerassistenz, wie zum Beispiel der adaptive Tempomat und der Spurwechsel- und Überholassistent, die bisher nicht nur aus der Entwicklungs-, sondern auch aus der Anwendungsperspektive als eigenständige Teilsysteme betrachtet wurden. Die erhöhte Bewertungskomplexität, die sich aus der notwendigen Permutation beliebiger Subsystemparametereinstellungen in Kombination mit Umwelteinflüssen ergibt, macht die effiziente Erkennung und Behebung sicherheitskritischer Systemfehler, die zum Beispiel durch Feature-Interaktionen entstehen, jedoch zu einer immer anspruchsvolleren Aufgabe.

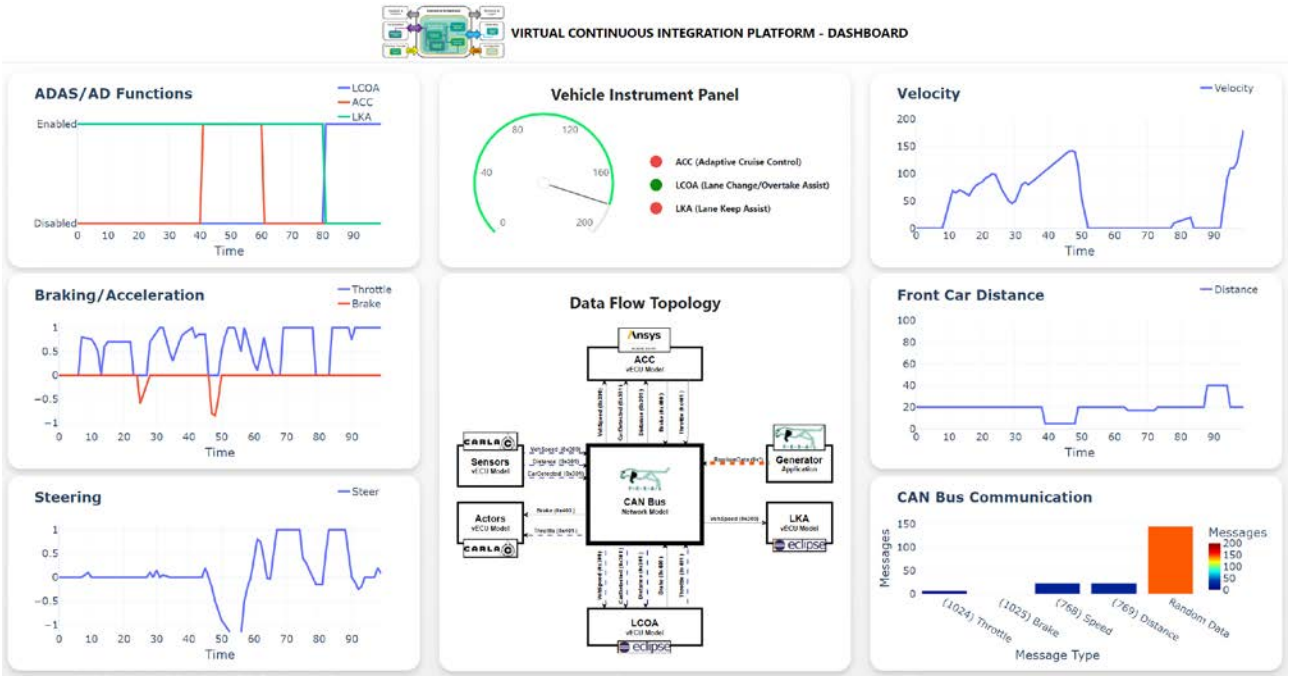


Abbildung 241: Dashboard zur Analyse von Simulationsergebnissen bzgl. relevanter Parameter und Eigenschaften des zu testenden Systems (©Fraunhofer).

Methode und Produktlösung

Mit der Absicht, die erforderlichen Verifikations- und Validierungstechniken auf reale Anwendungsfälle in der Praxis anwendbar zu machen, schlagen wir eine Lösungstechnologie vor, die es ermöglicht, hybride Prüfstände zu etablieren, um Gefahrenanalysen und Risikobewertungen auf der Grundlage virtueller kontinuierlicher Konstruktionsprinzipien, einheitlicher Schnittstellen und kompatibler Werkzeugketten durchzuführen - alles flexibel an die Besonderheiten des Anwendungsfalls anpassbar.

In diesem Zusammenhang stellen wir ein praxisnahes Produkt für die schnelle Evaluierung von ADAS-Funktionsdesigns vor, das auf der Referenz-architektur der Virtual Continuous Integration Platform (VCIP) [108] basiert. Es handelt sich dabei um ein integriertes virtuelles Testbed, das nach der CSCC-Methode (Continuous Shift-Left Convergence Concept) für die komplementäre Verkettung bewährter Modellierungs- und Simulationswerkzeuge mittels eines End-to-End-Kopplungsmechanismus [109] instanziiert wurde. Das Testbed besteht aus dem Simulations- und Integrationsframework FERAL, einem Funktionsmodellierungswerkzeug, einem Verkehrssimulator, automobilen Steuerungsmodulen sowie entsprechenden Schnittstellen, die ihre Bestandteile miteinander verbinden (Abbildung 242). Wir demonstrieren seine Anwendbarkeit für die virtuelle Validierung funktionaler Modellentwürfe, die drei populäre automatisierte Fahrfunktionen spezifizieren, anhand verschiedener Testszenarien, u.a. der Erkennung von Regressions- und Funktions-interaktionen während der Fehlerinjektion und des Funktionsintegrationstests. Anhand eines grafischen Auswertungs-Dashboards (Abbildung 241) werden die Simulationsergebnisse erläutert und Schlussfolgerungen zu ihrer Gültigkeit in Bezug auf die zu testenden Systemaspekte gezogen.

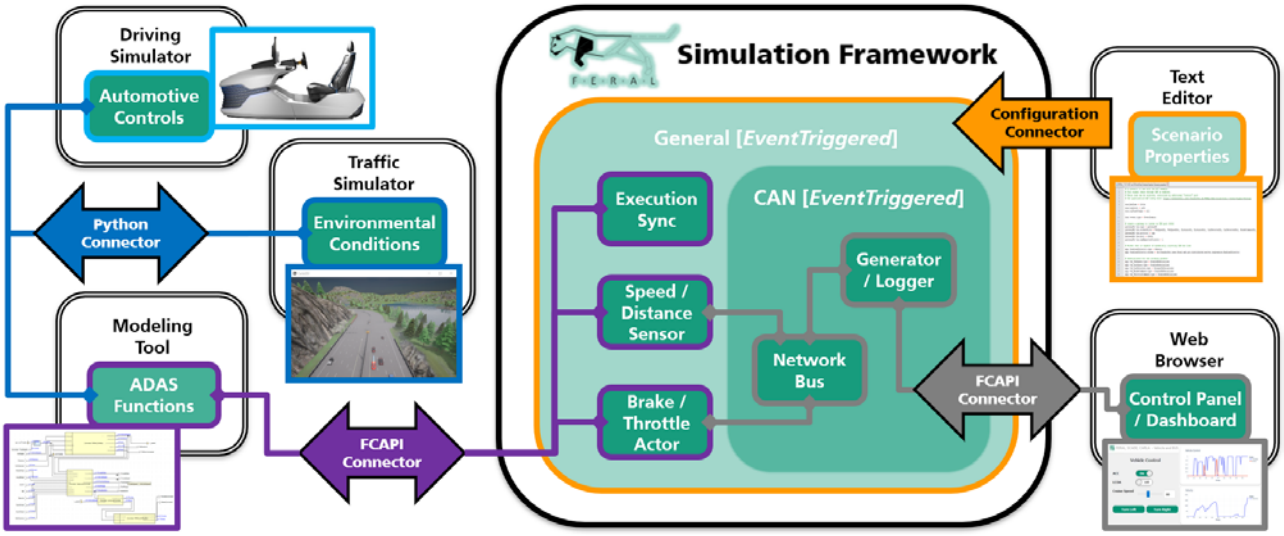


Abbildung 242: Instanziierung der VCIP-Referenzarchitektur mit interoperablen Werkzeugen für die systematische Bewertung hochautomatisierter Fahrfunktionen (©Fraunhofer)

3.1.2.7.3.11 Verteilte Testausführung

Durchgängige Testorchestrierung

Die Testorchestrierung ist als ein Prozess definiert, der zur Konkretisierung einer funktionalen Testspezifikation verwendet werden soll, indem das technische Design eines ADS, die Verfügbarkeit geeigneter Werkzeuge und Modelle pro Testinstanz und Kostenfunktionen bewertet werden. Das Ergebnis dieses Prozesses ist die technische Testspezifikation.

Um den V&V-Testprozess zu automatisieren, wird eine maschinenlesbare Darstellung der technischen Testspezifikationen benötigt. Darüber hinaus muss die Ausführung technischer Testspezifikationen auf verschiedenen Testinstanzen durchgängig und kontrolliert erfolgen.

Technische Testfallspezifikation

Im Rahmen des VVM-Projekts wurde von ZF eine DSL für technische Testspezifikationen entwickelt, die als JSON-Schema-basiertes Domänenmodell implementiert ist, das Testfälle beschreibt (siehe Abbildung 243).

Jeder Testfall besteht aus Verweisen auf eine Testinstanz, ein logisches Szenario, eine Variationsregel, die die Ableitung konkreter Szenarien aus logischen Szenarien ausdrückt, ein Device under Test, eine Reihe von Ersatzmodellen und auf während des Tests aufzuzeichnende Messgrößen, gegebenenfalls auch auf eine Beschreibung und Parametrisierung der Simulations-Engine.

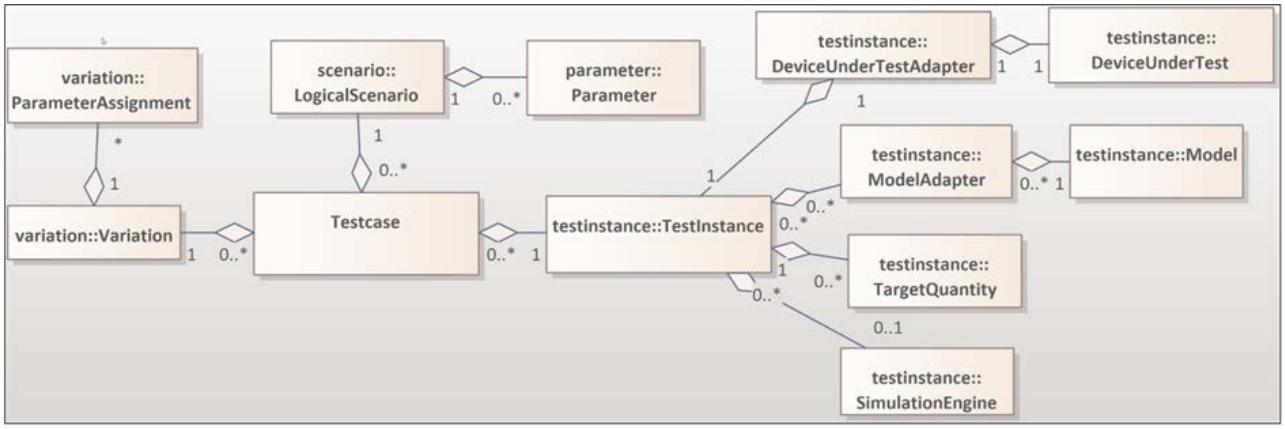


Abbildung 243: Domänenmodell der maschinenlesbaren technischen Testspezifikation

Framework zur Testausführung

Ein Framework zur Testausführung, das die eingehenden Testspezifikationen interpretiert, wurde als choreografierte Micro-Batch-Verarbeitungspipeline implementiert, die aus unabhängig skalierten (Post-) Prozessoren und einem abschließenden Aggregationsschritt besteht.

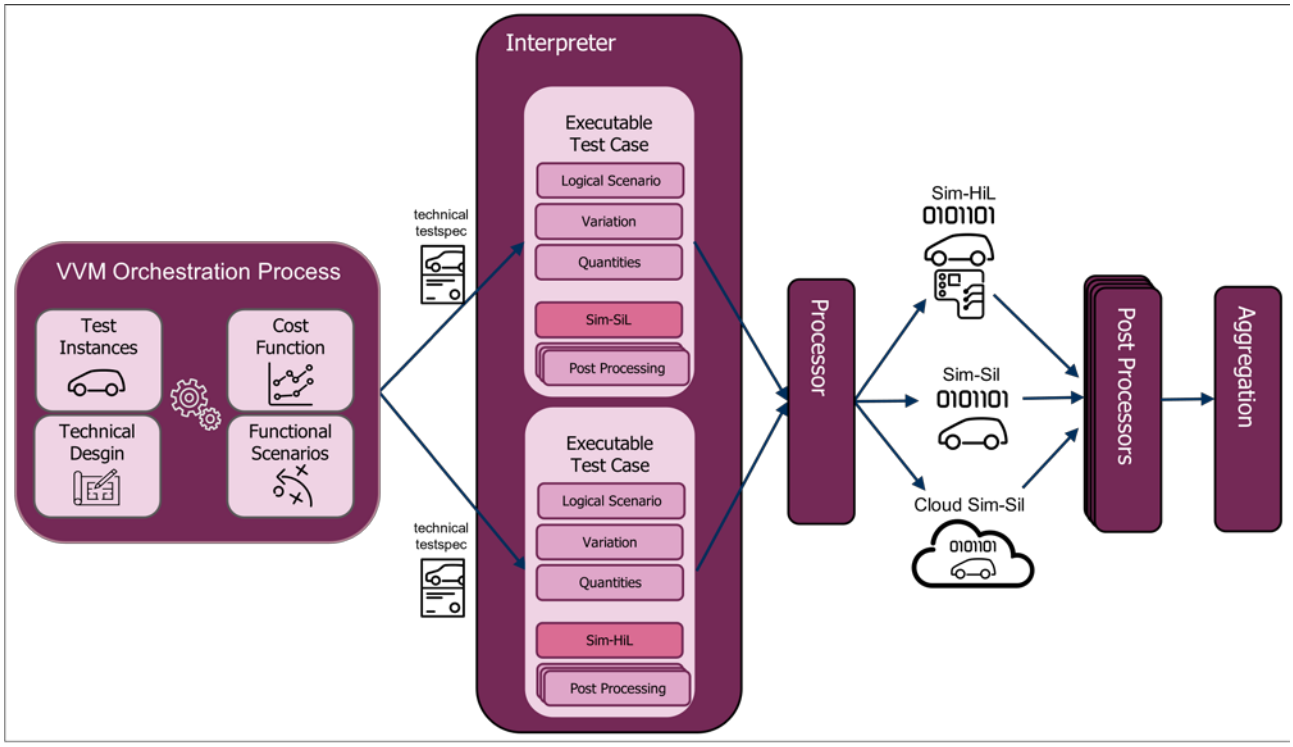


Abbildung 244: Framework zur Testausführung

Generische Schnittstelle für verschiedene Testinstanzen und Integration in Geschäftsprozesse

Durch die Beschreibung von Testaktivitäten als generische technische Testspezifikationen und durch die Bereitstellung eines agnostischen Frameworks zur Testausführung wird die durchgängige orchestrierte Nutzung verschiedener Testinstanzen ermöglicht, die lediglich auf das generische Framework zur Testausführung angepasst werden müssen. Aufgrund der ereignisbasierten Architektur des Frameworks ist eine Integration in verschiedene Geschäftsprozesse möglich, sei es der V&V-Prozess oder z.B. ein klassischer V-Modell-Ansatz.

3.1.2.7.3.12 Testexcecution

Konzept

Für hochautomatisierte Fahrzeuge ist ein umfangreicher Testprozess erforderlich, der von Funktionstests bis hin zu systematischen Tests unter realen Fahrbedingungen reicht. Um die Konsistenz zwischen diesen Tests, die sich in ihrem Abstraktionsgrad unterscheiden, zu gewährleisten, müssen sie gemeinsame Schnittstellen haben und weitgehend vergleichbar sein, d. h. eine Testpipeline mit verschiedenen Instanzen sollte nahtlos ineinander übergehen.

Abbildung 245 veranschaulicht ein Konzept, das Verkehrsdaten mit Hilfe einer intelligenten Testgebietsinfrastruktur erfasst, analysiert und auswertet. Mit diesen Informationen können spezifische Module eines hochautomatisierten Fahrzeugs in einer einfachen Open-Loop-Simulation bewertet werden, die dann in Form einer Closed-Loop-Simulation immer detaillierter und realistischer wird. Schließlich kann das System in realen Straßenszenarien getestet werden, während es gleichzeitig über die Infrastruktur des Testgebiets überwacht wird.

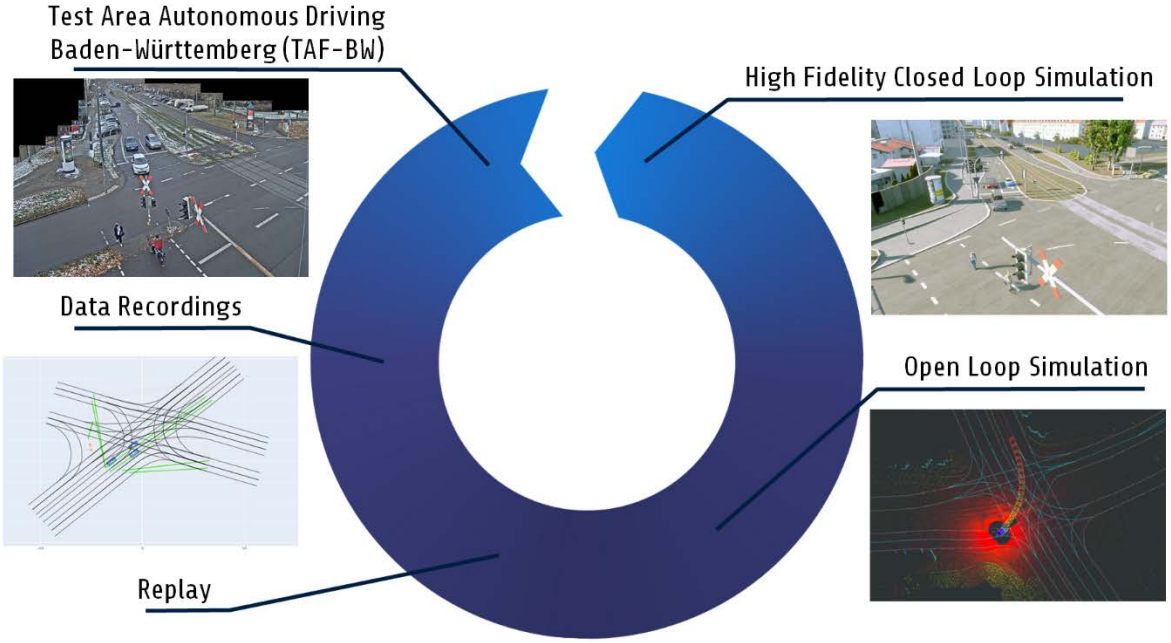


Abbildung 245: Konzept zum Testen hochautomatisierter Fahrzeuge in verschiedenen Testphasen

Aufzeichnung und Wiedergabe

Die Beobachtung authentischer Verkehrsszenen, einschließlich des Verhaltens der Verkehrsteilnehmer und der Umgebung, in der sie sich befinden, bildet die entscheidende Grundlage für die folgenden Analyseschritte. Auf dieser Basis können relevante Szenarien identifiziert und in der Simulation oder im Praxistest näher untersucht werden.

Simulation

Realitätsnahe Simulationen mit geschlossenem Regelkreis ergänzen reale Experimente und nicht-reaktive Protokollwiedergabe. Der bemerkenswerte Grad an Wahrnehmungs-, Verhaltens- und Inhaltsrealismus, der durch moderne modellbasierte und datengesteuerte Simulationen ermöglicht wird, erlaubt es, Tests auf besonders seltene oder kritische Szenarien zu skalieren, insbesondere solche, an denen VRUs beteiligt sind [110] [111].

Testfeld im öffentlichen Verkehr

Das Testfeld mit seiner Infrastruktur dient als Referenzmesssystem. Diese präzise, kalibrierte Messsensorik ermöglicht ein vertieftes Verständnis des Verkehrsgeschehens, das direkt vom SuT nicht möglich wäre. [112]. Neben der Überwachung der Sensoren des zu testenden Systems (z.B. Perzeptionsbewertung) wird im Testfeld auch das Gesamtverhalten des Systems bewertet [113]. Bewertungsmetriken geben Aufschluss darüber, wie der SuT in der aktuellen Umgebung abgeschnitten hat [112].

3.1.2.8 TP8 Datenbank

3.1.2.8.1 Einleitung

Das TP8 Datenbank stellt die Methodiken und Tools zur Ableitung von Szenarien aus Realdaten bereit, die für das Szenario-basierte Testen nach der in VVMethoden entwickeltem Vorgehen unerlässlich sind. Dies umfasst im ersten Schritt die Datenaufnahme in der realen Welt, welche zuerst die Daten in eine Rohdaten-Datenbank (Raw-Database) aufnimmt. Dies geschieht unter Berücksichtigung von Datenschutz-Aspekten in einem sogenannten Safety-Cage. Daten aus dieser Rohdatenbank werden anonymisiert, verlassen somit den Safety-Cage und können durch Labelling in Referenzdaten umgewandelt werden. Diese Referenzdaten werden in ein einheitliches Datenformat überführt, welches die automatisierte Verarbeitung durch die Datenbankautomatik (Advanced Scenario Engine) ermöglicht. Somit können Szenarien in Daten identifiziert und der Absicherungs- und Entwicklungsmethodik zugänglich gemacht werden. Während der Entwicklung der Methodik und der Prozesse sollte schon ein Austausch von Daten unter den Beteiligten möglich sein. Hierzu kann eine Entwicklungsdatenbank hilfreich sein. Diese ermöglicht auch den Austausch von Daten die (noch) nicht den Definitionen und Ansprüchen den Scenario Datenbank genügen und Entwicklung- und Weiterentwicklungs-Zwecken dienen. Einen Überblick über den beschriebenen Prozess verschafft die folgende Abbildung. In blau sind die Schritte des TP8 hervorgehoben.

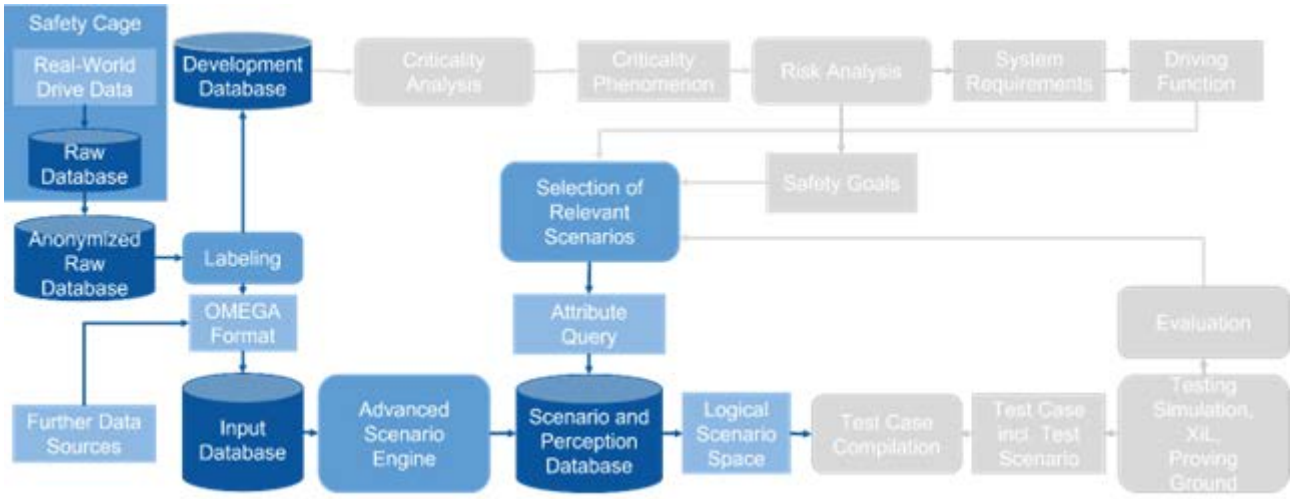


Abbildung 246 Überblick über den Datenfluss in VVMethoden

Die entwickelten Prozesse und Tools des TP8 sind detailliert im öffentlichen Deliverable D13 dokumentiert. Im Folgendem wird zuerst auf die der Szenariendatenbank und deren Kernbestandteile beschrieben. Im zweiten Abschnitt wird die Datenaufnahme, die Rohdatenbank und der Safety-Cage dargestellt. Zuletzt wird die Methode der Entwicklungsdatenbank präsentiert.

3.1.2.8.2 Szenariendatenbank

Grundlage der Entwicklung der Szenariendatenbank Methode sind die Ergebnisse aus E8.1a „Anforderungsanalyse an das Datenbankkonzept für den Use Case urbane Kreuzung“. Hieraus ergab sich insbesondere die Notwendigkeit einer Rohdatenbank und einer Entwicklungsdatenbank, welche in den auf diese Kapitel folgenden beleuchtet werden. In der Anforderungsanalyse konnten 38 User Stories definiert werden, aus denen die folgenden Prozesse zur Realisierung der Szenariendatenbank abgeleitet wurden: Schnittstellen-Definition, Szenarien-

Identifikation, Ausspielung der Szenarien und die Perzeptionsdatenbank. Diese werden im Folgendem näher erläutert.

Schnittstellen-Definition

Um Szenarien in Realdaten zu identifizieren ist eine Definition der Schnittstelle von Datenquellen und Datenbankmechanik essenziell (E8.1b „Schnittstellenbeschreibung von Inputdaten auf allen Layern“). Die Definition der Schnittstelle wurden durch die Entwicklung des OMEGA-Formats vollzogen (vgl. Kapitel 3.1.1.4 „Szenarienabstraktion Grundlagen (Realitätsabstraktion)“). Es umfasst alle 6-Ebenen des ebenfalls in VVMethoden weiterentwickelten 6-Ebenen-Modells. Analog zur Definition von Referenzdaten im OMEGA-Format können auch Perzeptionsdaten dargestellt werden. Hierbei ist die Beschreibung der Elemente durch die Selbst-Konfidenz-Werte der Perzeptions-Sensorik erweitert. Ebenfalls werden Informationen über den Sichtbereich und die verwendete Sensorik selbst mit abgespeichert. Die duale Darstellungsweise erfüllt die Erfordernisse zur Verknüpfung der Sensor- und Szenariendatenbank (E8.1d „Verknüpfung von Sensor und Szenariendatenbank“). Auf Basis des OMEGA-Format wird die einheitliche Uploadschnittstelle in die Datenbank definiert und umgesetzt (E8.1c „Definition einer einheitlichen Uploadschnittstelle zum Upload in die Datenbank“, E8.1f „Integration der einheitlichen Uploadschnittstelle“). Die Umsetzung erfolgt in Form einer REST-API und einer SQL-Datenbank. Zur Dokumentation der API wurde der Standard OpenAPI genutzt, welche eine einfache Umsetzung der API in verschiedenen Programmiersprachen zulässt und die Möglichkeiten der API ausführlich dokumentiert.

Szenarien-Identifikation

Ausgangspunkt für die Identifikation von Szenarien in Daten ist die Definition der Szenarien selbst. Diese Szenarien sollten den Anforderungen des Use Case urbane Kreuzung genügen und mit der Methodik zur Verifikation und Validierung automatisierter Fahrfunktionen harmonisieren (E8.1e „Berücksichtigung der Ontologie aus TP2, TP5 bei Erstellung des Szenarienkonzepts mit Fokus der Anforderungen des Use Case urbane Kreuzung“). Die in VVMethoden definierte Szenarienkonzept „Holistic Drving Scenario Concept for Urban Traffic“ erfüllt diese Kriterien (vgl. Kapitel 3.1.1.4 „Szenarienabstraktion Grundlagen (Realitätsabstraktion)“scroll-bookmark-180). Das Szenarienkonzept definiert 271 logische Szenarien-Klassen, sogenannten Basis-Szenarien, die das Egoverhalten und dessen Interaktion mit einem Verkehrsteilnehmer beschreiben. Zur Reduktion der Komplexität sind die Klassen so definiert, dass sie sich aus der Kombination von Sub-Konzepten ergeben. Durch die Aneinanderreihung und das parallele Ablaufen der Basis-Szenarien können längere Szenarien mit mehreren Teilnehmern beschrieben werden. Sie fungieren wie simple Bausteine aus denen komplexere Konstrukte zusammengesetzt werden können. Um an die Argumentation anzuknüpfen ist es wichtig, dass die Szenarien-Klassen und deren Identifikation in Realdaten ontologisch abgebildet werden können und mit den Konzepten der Kritikalitätsanalyse kompatibel sind. Dies wurde in VVMethoden dadurch erreicht, dass das OMEGA-Format zusammen mit der Ontologie A.U.T.O entwickelt wurde. So lassen sich Daten im OMEGA-Format in die ontologische Darstellung überführen und umgekehrt. Auch das Szenarienkonzept selbst ist über eine Ontologie definiert und knüpft an die bestehenden Ontologien an.

Durch die Datenbankmechanik können die Szenarien-Klasse in logische Szenarien-Instanzen überführt werden. Dazu müssen in Verkehrsdaten Szenarien identifiziert werden und aus den abgeleiteten Parametern der identifizierten Szenarien Parameter-Verteilung geschätzt werden. Da diese Parameter-Verteilungen den tatsächlich in der ODD auftretenden Verteilungen entsprechen

sollten (unter anderem um eine Risiko-Abschätzung zu ermöglichen), ist eine Verarbeitung von großen Mengen an Daten notwendig (Kapitel 3.1.1.5 „Szenarienabstraktion - Szenariobasiertes Testen“). Dies erfordert eine automatisierte Identifikation der Szenarien und eine automatisierte Berechnung derer Parameter, welche in TP8 konzeptioniert und prototypisch implementiert wurde (E8.2a „Konzeptentwicklung, Automatisierte Auswertung durch die Datenbankmechanik“ und E8.2c „Automatisierte Auswertung durch die Datenbankmechanik implementiert“). Dabei wurden die Methoden des PEGASUS-Projekts fortgesetzt und erweitert (E8.2b „Aufbau auf dem Konzept und den Erkenntnissen der PEGASUS-Datenbank“). Insbesondere die Adaption auf den urbanen Raum war hierbei eine Herausforderung.

Dadurch, dass sich die Basis-Szenarien aus der Komposition von Sub-Konzepten ergeben, lassen sich die Identifikations-Algorithmen effizient formulieren. So muss je Sub-Konzept ein Algorithmus definiert werden. Die Resultate der einzelnen Identifikationen können dann zu Basis-Szenarien aggregiert werden. Ebenso verhält es sich mit der Berechnung von Attributen und Parametern der Szenarien. Diese werden auch auf Ebene der Sub-Konzepte definiert und für die Basis-Szenarien kombiniert. Dieses Vorgehen reduziert die Komplexität des Problems und den Implementierungsaufwand der Lösung signifikant. Dadurch, dass sowohl die Eingangsdaten im OMEGA-Format als auch die Szenarien ontologisch verknüpft sind, kann eine Durchgängigkeit sichergestellt werden.

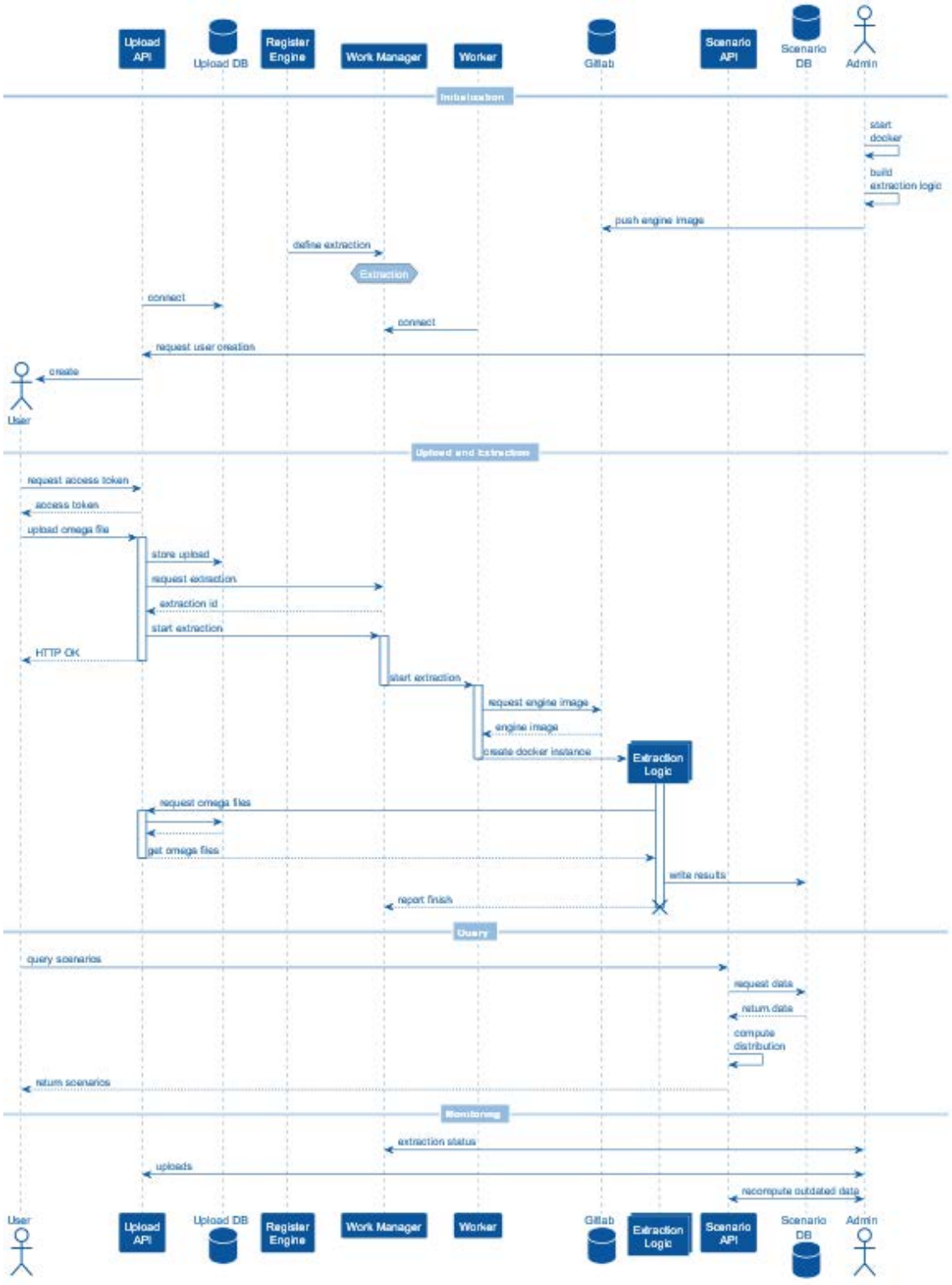


Abbildung 247 Interaktionsprozesse der Datenbankmechanik der Szenariendatenbank.

Nicht nur die Identifikation von Szenarien selbst, sondern auch die Verwaltung und das Auslösen des Identifikationsprozesses müssen automatisiert und skalierbar sein. Dazu wurde die Datenbankmechanik konzeptioniert und implementiert. Die obenstehende Abbildung 229 zeigt den Prozess-Ablauf der Szenariendatenbank mit den Agenten Benutzer, welcher Daten in die Szenariendatenbank einpflegt und Szenarien aus der Szenariendatenbank ausliest und dem Administrator, welcher die Datenbank betreibt. Nicht alle Aufgaben müssen vom gleichen Benutzer

ausgeführt werden. Es kann sich bei jedem Schritt auch um verschiedene Benutzer handeln. Die Bestandteile der Szenariendatenbank sind die Upload Datenbank, der Worker und die Szenariendatenbank. Die Upload Datenbank speichert die Verkehrsdaten im OMEGA-Format ab und stellt sie den Szenarien-Identifikations-Algorithmik (ASE) bereit welche von einem Worker nach erfolgreichem Upload automatisiert, ausgeführt wird. Die Ergebnisse werden in die Szenariendatenbank geschrieben. Sowohl die Upload Datenbank als auch die Szenariendatenbank stellen eine API zum Authentifizieren bereit und interagieren mit den Datenbanken. Dies ist deswegen wichtig, da eine große Menge an Daten verarbeitet werden muss und dies nur voll automatisiert praktikabel ist.

Um die Argumentation und die Validierung und Verifikation Prozesse unterstützen zu können ist es wichtig, dass die Herkunft von Szenarien und die angewendeten Prozesse nachvollziehbar und wiederholbar bleiben. Zu jedem Szenario in der Szenariendatenbank kann die verwendete Algorithmik und deren Parametrisierung und die Quelldatei in der Eingangsdatenbank, sowie der Uploader bestimmt werden. Dies ermöglicht, dass Szenarien, die mit z.B. fehlerhaften Parametrisierungen in der Szenarien-Extraktion erstellt wurden, identifiziert und korrekt neu berechnet werden können.

3.1.2.8.3 Ausspielung von Szenarien

Sind ausreichend Verkehrsdaten durch die Szenariendatenbank verarbeitet worden, so können wie in Kapitel 3.1.1.5 „Szenarienabstraktion - Szenariobasiertes Testen“ beschrieben logische Szenario Instanzen gebildet werden. Diese müssen den Test-Verantwortlichen zugänglich gemacht werden. Dies geschieht über das OpenSCENARIO Format. Samples aus den logischen Szenarien können in verschiedenen Abstraktionsstufen in OpenSCENARIO überführt werden (Replay to Simulation (RtS), Advanced Replay to Simulation (ARtS), Basis-Szenario, Kombiniertes Szenario, Kombiniertes Szenario + ARtS). Beispiel einer solchen Ausspielung ist in der folgenden Abbildung zu sehen. Hierbei handelt es sich um eine RtS Ausspielung im Simulator esmsini.

Abbildung 248 Screenshot einer beispielhaften Ausspielung eines Szenarios über OpenSCENARIO im Simulator esmini

Bei der Bewertung eines ADS ist der Tester nicht zu jedem Zeitpunkt an allen Daten interessiert, sondern möchte sich auf bestimmte Aspekte konzentrieren. Dies gilt auch für die Entwicklung von ADS. Daher erfordert die Datenbank eine Filterfunktion, die es dem Benutzer ermöglicht, sich auf das Wesentliche in der Situation und unter Berücksichtigung der ODD zu konzentrieren. Deswegen bietet die Szenariendatenbank Funktionen zur Filterung der Szenarien basierend auf allen Ebenen des 6-Ebenen-Modells. Dies umfasst die Szenarienklassen, Parameter und Attribute der Szenarien, Eigenschaften des Straßennetzes und Wetterbedingungen. Die Filterfunktionen

können durch ein Web-Interface bedient werden und werden automatisch in Datenbank-Queries übersetzt. So kann die für den Anwender relevante Teilmenge der Basis-Szenarien in der Szenenariendatenbank identifiziert werden. Nicht nur einzelne Basisszenarien, sondern auch bestimmte Abfolgen dieser können von Interesse sein. Auch nach diesen kombinierten Szenarien kann durch ein Web-Interface gesucht werden. Dazu wurde eine Graphen-basierte Anwendung konzipiert und implementiert, die es dem Anwender erlaubt beliebige Abfolge und Relationen von Basis-Szenarien und Events zu formulieren. Ein Beispiel so einer Anfrage ist in folgender Abbildung zu sehen.

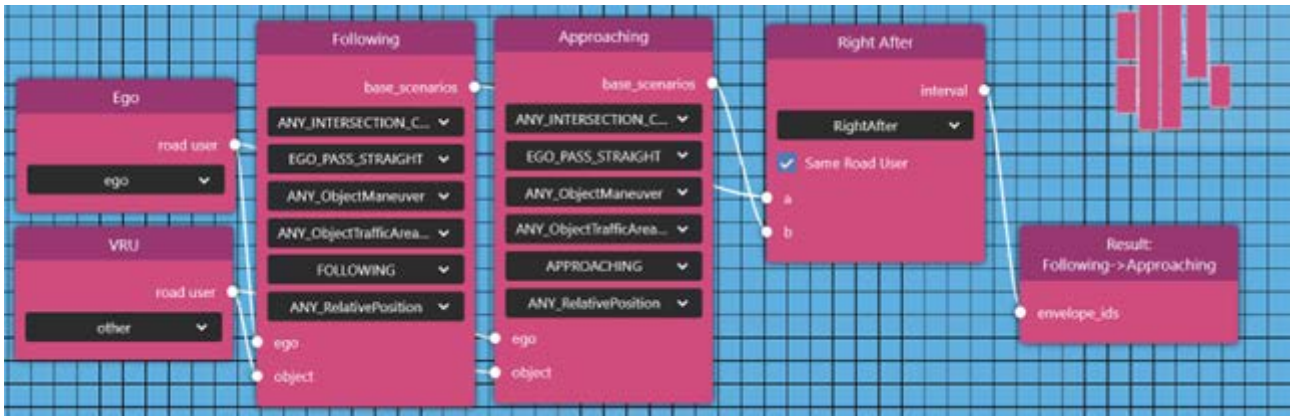


Abbildung 249 User Interface zum Filtern und Suchen von relevanten Szenarien

Neben dem Suchen selbst, bietet das Interface der Szenariodatenbank auch diverse graphische Aufbereitungen des Inhaltes der Datenbank und der gesuchten Teilmenge daraus. Dies ist wichtig, um den Anwender einschätzen zu lassen, ob seine Anfrage seinen Erwartungen entspricht. Neben allgemeinen Statistiken lassen sich auch die auftretenden Parameterverteilungen der logischen Szenarien Instanzen betrachten.

Perzeptionsdatenbank

Die Leistungsfähigkeit von ADS hängt stark von den Fähigkeiten der Sensorwahrnehmung ab. Daher ist die Identifikation systematischer Fehler in der Wahrnehmung von großer Bedeutung. Zu diesem Zweck wurde eine Perzeptionsdatenbank (Sensordatenbank) entwickelt. Da die Referenzdaten nur in Form von Objektlisten vorliegen, müssen die Sensordaten ebenfalls in Objektlisten transformiert werden. Das Datenformat der Wahl ist das OMEGA-Format. Zusätzlich zu jedem Wert wird das Selbstvertrauen des Wahrnehmungsmodells, das die Objektliste erstellt, abgespeichert. Die Perzeptionsdaten im OMEGA-Format können dann in die Perzeptionsdatenbank hochgeladen und automatisiert ausgewertet werden. Während der Analyse werden verschiedene Metriken zur Objekterkennung und -verfolgung berechnet. Beispiele sind MOTA (Multiple Object Tracker Accuracy), Recall und F1-score. Dabei wird die Perzeptionsdatei mit der entsprechenden Referenzdatei in der Szenariendatenbank verknüpft, was notwendig ist, um die Perzeptionsqualität zu evaluieren. In der Umsetzung ist Szenariendatenbank und Perzeptionsdatenbank technisch nicht getrennt und stellt somit sicher, dass Referenz-, Perzeptions- und Szenarien-daten in Relation gesetzt sind (E8.1d „Verknüpfung von Sensor und Szenariendatenbank“).

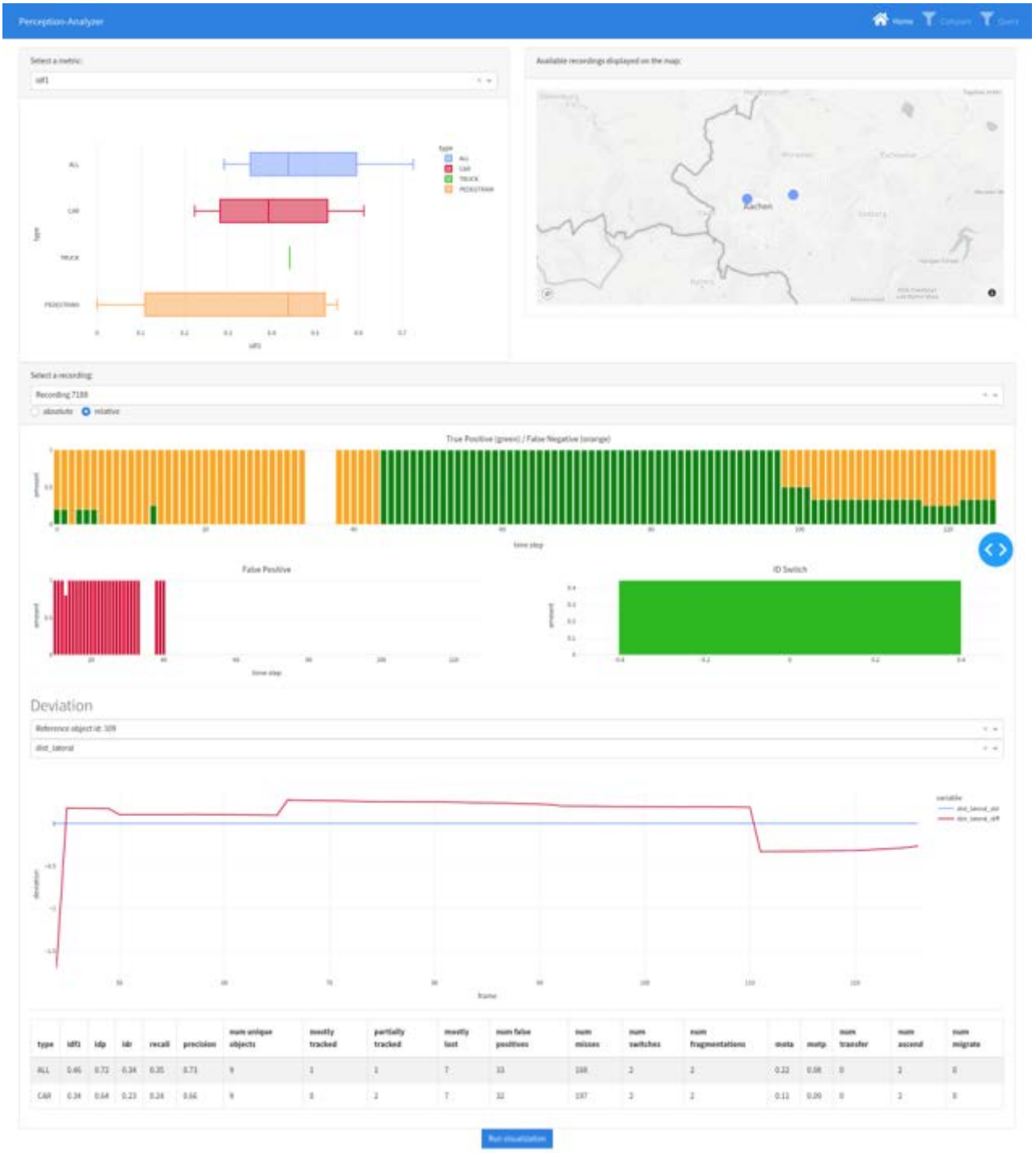


Abbildung 250 User Interface der Perzeptionsdatenbank

Die obige Abbildung 250 zeigt das User Interface der Perzeptionsdatenbank mit exemplarischen Ergebnissen einer solchen Analyse. In den dargestellten Daten werden künstliche Wahrnehmungsdaten (durch Hinzufügen von Rauschen) verwendet, da zum Zeitpunkt der Analyse keine anderen Daten verfügbar waren. Anhand dieser Schnittstelle kann ein Nutzer die Leistung des Wahrnehmungssystems visuell überprüfen. Durch eine Aufschlüsselung nach Aufnahmezeit können problematische Zeiträume identifiziert werden. Filteroptionen ermöglichen die Spezifizierung des Betriebsbedingungenkatalogs (ODD, Operational Design Domain) (z.B. Betrachtung von Daten nur bei starkem Niederschlag), um sich auf die relevanten Aspekte zu konzentrieren.

3.1.2.8.4 Entwicklungsdatenbank

Im Rahmen von VVMethoden wurden über 15.000 Objekte in die Entwicklungsdatenbank COSCINE geladen. Dies bestärkt die Bedeutung einer Entwicklungsdatenbank bei der Entwicklung geeigneter Methoden. Aber auch bei der Anwendung von Methoden kann eine Entwicklungsdatenbank eine Rolle spielen. So können dort schon Daten ausgetauscht werden, bevor sich deren Struktur gefestigt hat und in andere Datenbanken aufgenommen werden kann. Coscine ist eine Lösung, die ein FAIR-Datenmanagement ermöglicht (Findable, Accesssible, Interoperable, Reusable). Es umfasst den gesamten Forschungsdaten-Lebenszyklus und bietet eine umfangreiche Verwaltung von Metadaten. Die Metadaten werden durch Anwendungsprofile definiert, die detaillierte Datenattribute (z.B. Szenario Typen und Kritikalitätsphänomene) festlegen und es ermöglichen Daten in Relation zu anderen Daten zu stellen. Dabei werden W3C-Standards wie RDF und SHACL verwendet. Persistent Identifikatoren ermöglichen eine eindeutige und beständige Verlinkung der Objekte. Die Integration von ElasticSearch ermöglicht das schnelle Finden der gesuchten Daten. Der Workflow mit COSCINE ist in der folgenden Abbildung dargestellt.

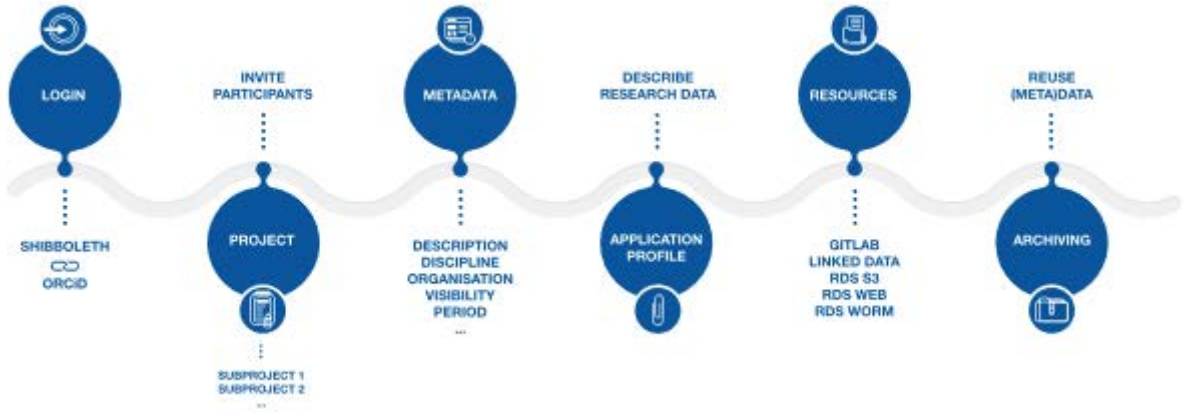


Abbildung 251: Workflow in Coscine

Im Rahmen von VVMethoden wurde COSCINE weiterentwickelt und als Entwicklungsdatenbank mit 8TB Speicher den Projektpartnern zu Verfügung gestellt. Diese Daten sind durch eine langfristige Archivierung den Projektpartnern auch nach Projektende noch zugänglich. Insbesondere wurden Anwendungsprofile für die Bedürfnisse von VVMethoden entwickelt. Ein Beispiel ist das „inD VVM“- Anwendungsprofil, welches die Verkehrsdaten aus dem inD-Datensatz mit den erfassten Szenarien, Sensorwerten und dem Fahrzeugverhalten ergänzt. Ebenso lassen sich Kritikalitätsphänomene annotieren. Insgesamt hat sich Coscine als ein wertvolles Werkzeug für das Datenmanagement im VVMethoden und darüber hinaus bewiesen. Es fördert die Einhaltung der FAIR-Prinzipien und unterstützt die Entwicklung des autonomen Fahrens durch effiziente Verwaltung komplexer Forschungsdaten.

3.1.2.8.5 Aufnahme von Referenzdaten

Ein der Herausforderungen des Projektes war die Aufnahme von Referenz-Daten, um die FUC und deren Kritikalitätsphänomen in der realen Welt zu beobachten und zu analysieren. Dazu wurde eine Referenz-Sensorik definiert, welche aus den Kritikalitätsphänomenen, dem Verkehrsteilnehmer Verhalten und der gegebenen Infrastruktur aus den FUC abgeleitet wurde. Hierbei wurde stets der Worst-Case angenommen um eine Abschätzung auf der sicheren Seite zu

gewährleisten. Das daraus resultierende AVL Dynamic Ground Truth System ist in der untenstehenden Abbildung zu sehen.

Abbildung 252 Referenzdaten-Sensorik

3.1.2.8.6 Verwaltung von Referenzdaten

Die Aufnahme der Referenz und SUT Daten erfolgt in drei Schritten: Der Online-Fahrzeugverarbeitung, der Offline-Datenreduktion und der Rohdatenbank. Bei der Online-Fahrzeugverarbeitung wird ein Tagging implementiert, welches es dem Anwender ermöglicht relevante Situation zu benennen und für die weitere Verarbeitung zu markieren. Die so bestimmten Situationen werden mitsamt der Sensor-Informationen der Referenz und SUT Sensoren abgespeichert. Nach einer Aufnahmefahrt fließen sie in eine Offline-Datenreduktion. Diese identifiziert relevante Ereignisse mithilfe von Algorithmen und Methoden der statistischen Analyse, um relevante Zeitspannen zu bestimmen, die in die Rohdatenbank hochgeladen werden. Neben den Rohdaten selbst, stellt die Rohdatenbank Datenmarkierung, Datenmanagement, Offline-Perzeption und Datensuche bereit. Daten welche unter die Datenschutz-Grundverordnung (DSGVO) fallen werden nur im sogenannten Safety-Cage bereitgestellt. Dies ist ein Teil der Datenbank der einen besonders restriktive Zugriffsrechte und eine ausführliche Zugriffsdokumentation aufweist. Bevor die Rohdaten weiter verteilt werden, werden die Privatsphäre relevanten Aspekte der Daten anonymisiert und pseudonymisiert. Diese nunmehr unbedenklichen Daten können dann ins Labelling fließen und in das OMEGA-Format umgewandelt werden. Kernaspekte der Verwaltung der Referenzdaten sind:

1. Aufnahme der Ground Truth und SUT Rohdaten mit den zugehörigen Fahrzeugdaten und Metadaten.
2. Automatischer Workflow zum Umwandeln der Rohdaten in die definierten Formate und Strukturen.
3. DSGVO konforme Datenspeicherung der nicht anonymisierten Daten im Safety-Cage und Speicherung der anonymisierten Daten.
4. Rollen basierte Zugriffsberechtigungsverwaltung mit Minimierung von Berechtigungen, angepasst an die Rolle der Projektpartner.
5. Suchmaske zum Finden von Rohdaten anhand von Metadaten.
6. Szenario Daten Interface um den Export in die VVMethoden Szenariendatenbank (über das OMEGA-Format) zu ermöglichen.

In folgender Abbildung ist die gesamte Architektur der SUT und Referenzdaten Rohdatenbank zusammengefasst:

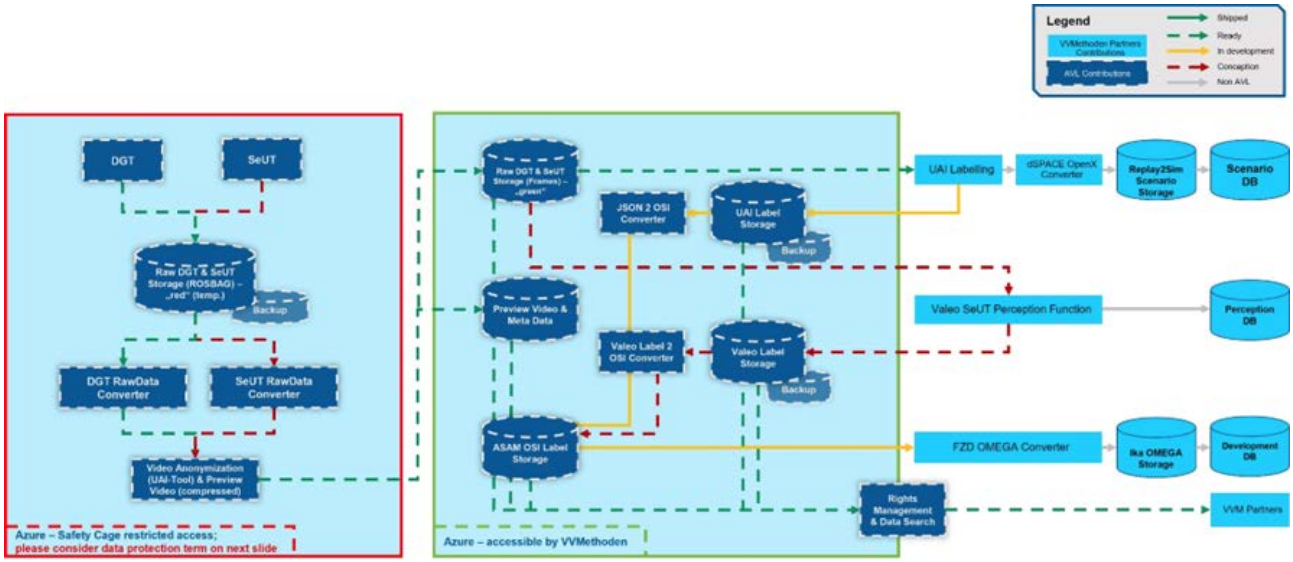


Abbildung 253 Architektur der Sensor- und Referenz- Rohdatenbank.

3.1.2.8.7 Zusammenfassung

Das TP8 hat eine Methodik konzeptioniert und implementiert, die ein ODD (Operational Design Domain) anhand logischer Szenarien mit Hilfe einer Szenariodatenbank modellieren kann. Durch die Ableitung aus dem 6-Schichten-Modell und Ontologien wurde ein Szenarien-Konzept erstellt, das zur Abdeckung einer spezifizierten ODD konzipiert ist.

Das Szenarienkonzept beschreibt die Dynamiken des Verkehrs durch Bausteine, den Basisszenarien. Diese definieren die Beziehung und das Verhalten des Ego-Objekts zu einem anderen Objekt. Für jedes dieser Basisszenarien werden Parameter festgelegt, wodurch logische Szenarien entstehen. Basierend auf diesen Szenarien werden Vollständigkeits- und Abdeckungsargumente aufgebaut. Komplexere und längere Szenarien können durch die Kombination der Basisszenarien, sogenannte kombinierte Szenarien, erstellt werden. Samples aus den logischen Szenarien können in verschiedenen Ebenen in OpenSCENARIO konvertiert werden. Das Ergebnis der Szenarien-Erstellung kann zur Formulierung von Testfällen verwendet werden.

Um Parameterverteilungen für die Instanzen logischer Szenarien zu erhalten, die die gewünschte ODD widerspiegeln, wird eine Szenariodatenbank verwendet. Zunächst benötigt die Szenariodatenbank Daten, die in der realen Welt erfasst wurden und die ODD widerspiegeln. Das TP8 hat einen Prozess entwickelt, wie solche Daten erfasst und durch Labelling in Referenzdaten umgewandelt werden. Datenschutzprobleme werden durch das Konzept eines Safety-Cages adressiert. Die objektlistenbasierten Referenzdaten werden im neu definierten OMEGA-Format gespeichert, das als Schnittstelle zwischen Szenariodatenbank und Datenquellen fungiert und mit einer Ontologie verknüpft ist, um die Argumentation zu unterstützen. Basierend auf diesen Daten kann die Szenariodatenbank Szenarien und deren Parameter identifizieren, aus denen die Instanzen logischer Szenarien abgeleitet werden. Zusätzlich werden Attribute und Ereignisse berechnet, die bei der Filterung der Szenarien auf die relevanten helfen.

Während der Entwicklung dieser Methoden und der Erstellung von Szenariendatenbank ist der Datenaustausch zwischen den beteiligten Parteien notwendig. Dieses Problem wird durch eine Entwicklungsdatenbank gelöst. Sie ermöglicht den Austausch von Daten mit Metadaten auf nachvollziehbare Weise.

Zusammenfassend präsentiert das TP8 eine Methodik und demonstriert praktisch, wie logische Szenarien definiert und Parameterverteilungen erworben werden können, die eine ODD modellieren. Damit wird die Entwicklung und Validierung von Fahrerassistenzsystemen (ADS) unterstützt.

3.1.2.9 TP9 Prozess Instanziierung, Anwendung

3.1.2.9.1 Zielsetzung

Eine zentrale Aufgabe des Teilprojektes 9 ist die Sammlung und Bündelung der Anforderungen der Industriepartner, sowie die Rückführung der daraus gewonnenen Erkenntnisse an die Industriepartner. Insbesondere werden im Teilprojekt 9 die Anforderungen und Erkenntnisse der Industriepartner gesammelt, die inhaltlich nicht direkt an den Teilprojekten 1 bis 8 beteiligt sind, deren Anforderungen jedoch ebenfalls in das Projekt einfließen sollen („Brückenfunktion“). Dies beinhaltet auch die Anforderungen seitens der regelungsnahen Institutionen, mit besonderem Blick auf die Eignung automatisierter Fahrzeugsteuerungsfunktionen zur sicheren Führung eines Kraftfahrzeuges im Straßenverkehr. Die Sammlung und Aufbereitung der industriellen Anforderungen für den Anwendungsfall urbane Kreuzung erfolgt dabei in Workshop zusammen mit den Industriepartnern. In der ersten Phase des Projektes werden zunächst die initialen Anforderungen der Industriepartner bezüglich des Anwendungsfalls der „urbanen Kreuzung“ von den Industriepartnern eingesammelt, aggregiert und aufbereitet.

Das Ziel der übergreifenden „Brückenfunktion“ im Projekt ist zum einen die Sicherstellung, dass alle Industriepartner den gleichen konsistenten Stand der Erkenntnisse erhalten, um diesen firmenintern nutzen zu können, auch wenn sie nicht direkt an den Arbeitspaketen 1 bis 8 beteiligt sind. Eine vereinzelte Erprobung unterschiedlicher Stände wird so vermieden, die Anwendbarkeit der Industrieergebnisse in der Breite sichergestellt. Zum anderen sollen die Erkenntnisse der Industriepartner aus dem Teilprojektes 9 gebündelt und konsolidiert an das Projekt übergeben werden, um so sicherzustellen, dass die Anforderungen und Erkenntnisse der Industriepartner in die Arbeitspakete einfließen.

Das Teilprojekt 9 sammelt und identifiziert darüber hinaus die bei den Industriepartnern eingesetzten Werkzeuge, Werkzeugschnittstellen und Dateiformate, sowie mögliche Anforderungen an die Werkzeuge, Werkzeugschnittstellen und Dateiformate der Absicherungsketten bzw. der Testumgebung für den Anwendungsfall Urbane Kreuzung. Zudem erfolgt eine Harmonisierung der Schnittstellen innerhalb der VVM-Methode.

Übergreifend wird im Teilprojekt 9 ein durchgängiges Baselining durchgeführt, das sicherstellt, dass zum einen eine Nachverfolgbarkeit der Prozesse und Methoden usw. möglich ist. Zum anderen, soll durch das Baselining sichergestellt werden, dass alle Partner stets auf dem gleichen Stand der aktuellen Prozesse, Methoden, etc. arbeiten. Das übergreifende Baselining wird vom TP1 in Kooperation und Abstimmung mit dem TP9 durchgeführt.

Das Teilprojekt 9 trägt damit zur Qualitätssicherung und zur Erhöhung der Marktakzeptanz der Ergebnisse jedes Teilprojektes implizit bei. Die Brückenfunktion und die transparente Nachverfolgbarkeit („Traceability“) der Ergebnisse wird durch das Baselining-Tool aus Teilprojekt 1, sowie durch die SysML-basierte Dokumentation der Gesamtmethode unterstützt, wodurch zum einen das Projektmanagement erleichtert, und zum anderen die sichere Nachvollziehbarkeit der Ergebnisse erreicht wird. Dabei koordiniert das Teilprojekt 9 die kontinuierliche Weiterentwicklung und Verbesserung des Modells und der Implementierung sowie die Harmonisierung der innerhalb der VVM-Gesamtmethode erstellten Prozesse und Artefakte in enger Zusammenarbeit und Abstimmung mit den Projektpartnern. Das Teilprojekt 9 trägt wesentlich zur Validierung und Akzeptanz der Methode und zum hierarchischen Herunterbrechen der Methodenbausteine, sowie zum Zusammenfügen der Ergebnisse innerhalb einer durchgängigen Sicherheitsargumentation bei.

Für das Teilprojekt 9 hat PROSTEP die Teilprojektleitung übernommen.

3.1.2.9.2 Anforderungserhebung

Neben dem eingangs dargestellten generellen und übergeordneten Ziel, verfolgt das Vorgehen zur Anforderungserhebung im VVMethoden-Projekt noch weitere Ziele. Zum einen soll durch dieses Vorgehen der firmeninterne Austausch innerhalb der beteiligten Fachabteilungen gefördert und ein Bewusstsein für die jeweiligen aktuellen Stände, eingesetzten Tools, verwendeten Methoden und Prozesse der Abteilungen geschaffen werden. Zum anderen soll ein gemeinsames Bild, der teils innerhalb der Abteilungen unterschiedlichen Erwartungen an und Ziele für das VVMethoden-Projekt erarbeitet werden.

Diese gemeinsame Erarbeitung soll auch das Problembewusstsein und -verständnis unter den Beteiligten über Abteilungsgrenzen hinweg fördern. Darüber hinaus können die Inhalte des auf diesem Wege erzeugten Zielbildes auch für die partnerübergreifende Anforderungserhebung genutzt werden. Eine anschließende Anonymisierung und partnerübergreifende Priorisierung stellt sicher, dass die maßgeblichen Anforderungen auch ohne Einschränkung von allen Projektpartnern genutzt werden können. Abbildung 254 zeigt schematisch das gesamte im VVM-Projekt durchgeführte Vorgehen zur Ermittlung der industriellen Anforderungen von deren Erhebung bis zu ihrer Priorisierung.

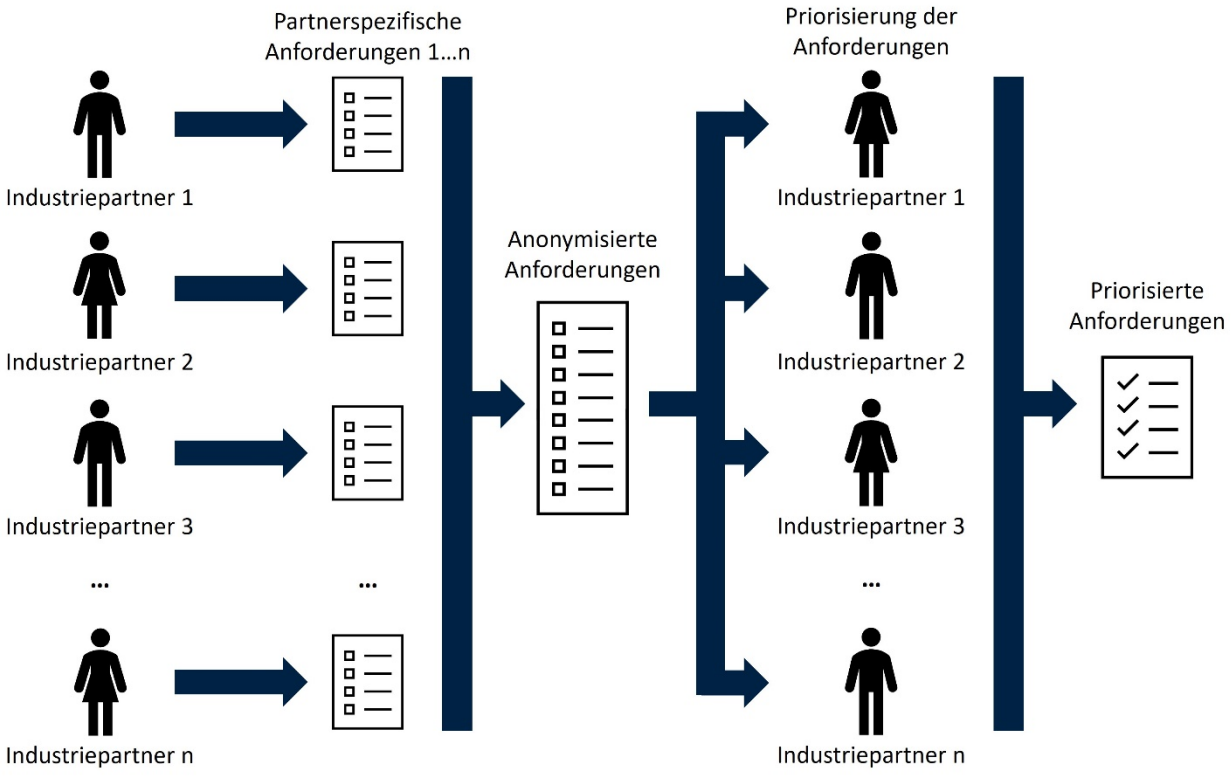


Abbildung 254: Vorgehen zur Ermittlung von Anforderungen die aus Industriesicht eine hohe Priorität haben

Im Rahmen der Vorbereitung der Industrieworkshops im VVMethoden-Projekt wurde entschieden für die Dokumentation und interne Aufbereitung der Ergebnisse ein modellbasiertes Vorgehen zu nutzen.

Dies verfolgt die folgenden Ziele:

- Gewährleistung eines einheitlichen Vorgehens über alle beteiligten Partner.
- Ein einheitliches Vorgehen verbessert die Vergleichbarkeit und Konsistenz der Ergebnisse.
- Strukturierter Bezug zu aktuell angewendeten Entwicklungsartefakten vereinfacht die Formulierung von Anforderungen.
- Strukturiertes und geleitetes Vorgehen erleichtert den Partnern sowie den Interviewenden die Anforderungsaufnahme.
- Eine strukturierte Aufnahme der Anforderungen, nach einem vordefinierten Vorgehen erleichtert die spätere Auswertung.
- Zusammenhänge und Abhängigkeiten können klar dargestellt, dokumentiert und visualisiert werden.

Abbildung 255 zeigt schematisch die von PROSTEP entworfene modellbasierte Methodik zur Aufbereitung der Workshops unter Einbeziehung verschiedener Partner und Fachabteilungen in den Häusern. Der Abbildung ist zu entnehmen, dass bei diesem Vorgehen, die bei den Partnern angewendeten und eingesetzten Methoden, Prozesse, Modelle, Tools und Schnittstellen aufgenommen und durch Relationen in Beziehung gesetzten werden (vgl. „Prozess A nutzt Tool A“). In dieser Darstellung ist aus Übersichtlichkeits- und Verständnisgründen, da hier kein SysML-Wissen vorausgesetzt werden sollte, auf die Abbildung der Anforderungen verzichtet worden, da sie prinzipiell an jedem Entwicklungsartefakt „hängen“ können.

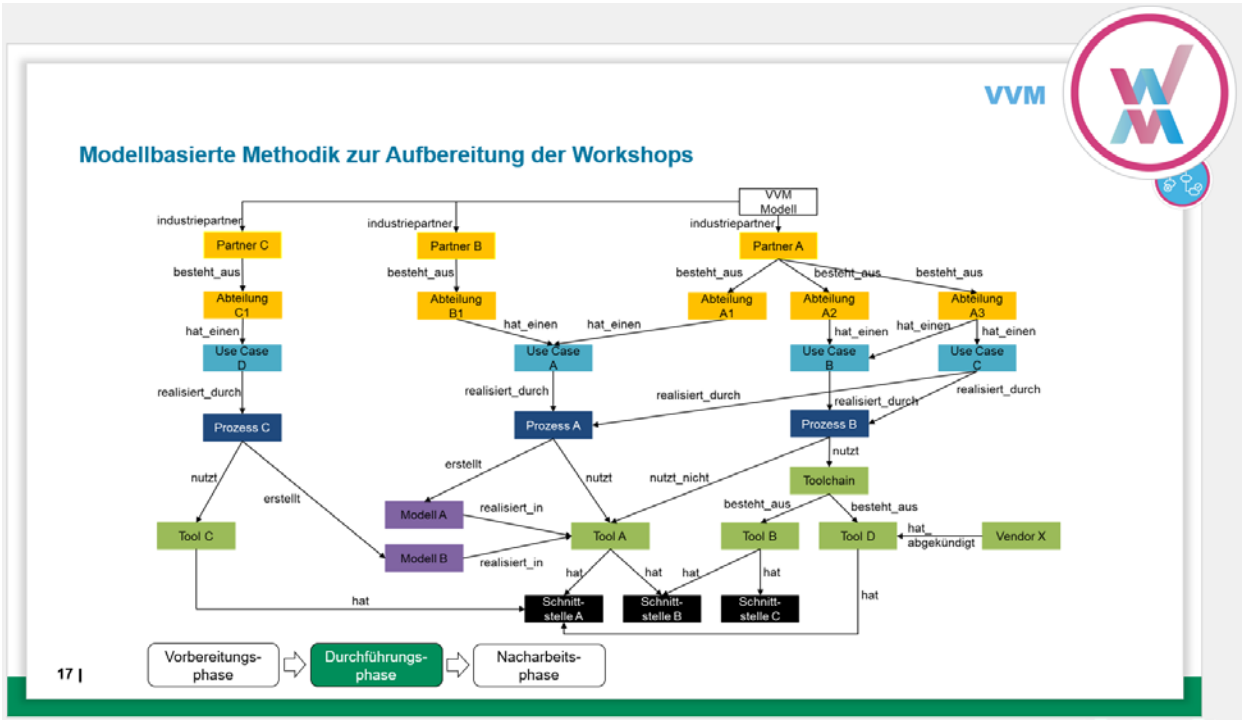


Abbildung 255: Modellbasierte Methodik zur Aufbereitung der Workshop.

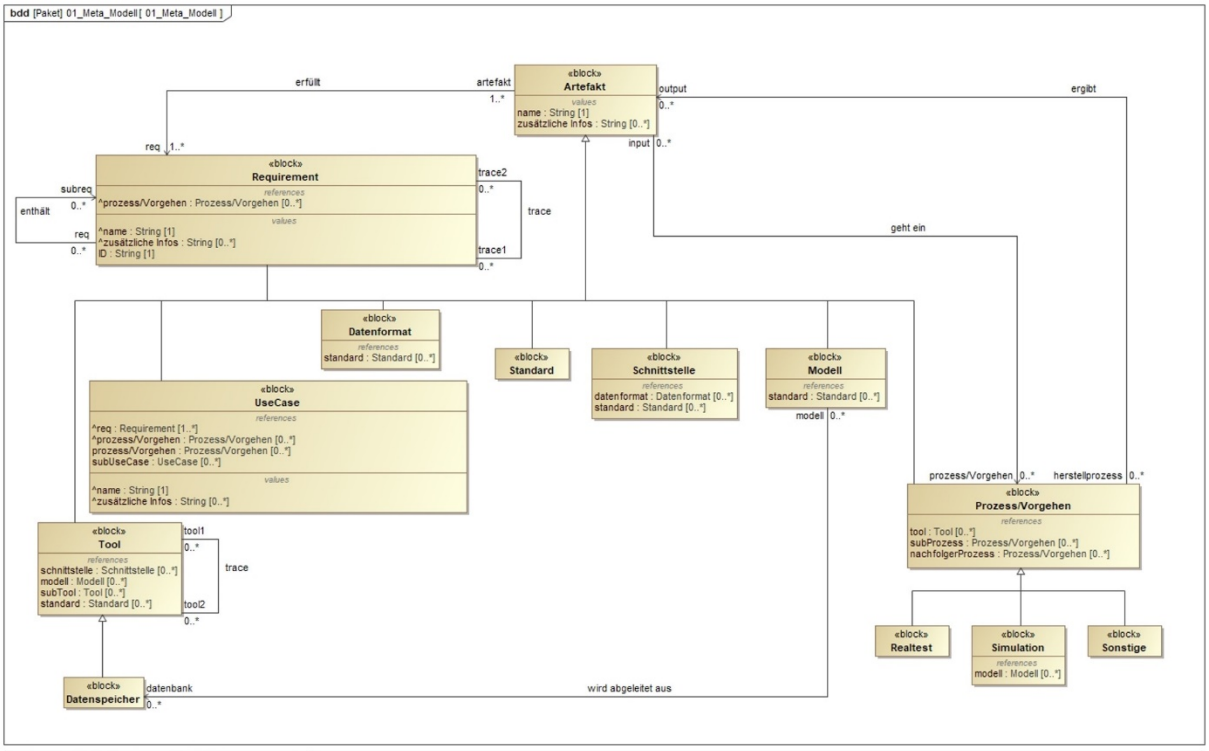
Für die konkrete Aufbereitung und Dokumentation der Ergebnisse der VVM-Industrieworkshops wurde von PROSTEP ein partnerübergreifendes SysML-Modell aufgebaut. Das dem Modell zugrunde liegende Metamodell, dass für alle Partner gleichermaßen angewendet wurde, ist in Abbildung 256 abgebildet. Sie zeigt dabei zwei separate sich ergänzende Diagramme, die das Metamodell der Auswertung und Dokumentation in SysML beschreiben.

Im oberen Diagramm wird der Zusammenhang zwischen den Entwicklungsartefakten und den Anforderungen definiert. Die Vererbungsbeziehung in der Mitte des Diagramms bezieht sich direkt auf die Entwicklungsartefakte Tool, Use Case, Datenformat, Standard, Schnittstelle, Modell und Prozess/Vorgehen. Durch die „erfüllt“-Beziehung zwischen dem vererbenden Objekt „Artefakt“ und dem Requirement sind somit diese Entwicklungsartefakte direkt mit den Requirements verknüpft. Auch die eine Ebene tiefer, unter Tool bzw. Prozess/Vorgehen liegenden Entwicklungsartefakte erben direkt diese Beziehung. Somit ist es möglich, die oben angesprochene und in Abbildung 255 vernachlässigte Beziehung zwischen Entwicklungsartefakten und den zugehörigen Anforderungen übersichtlich im Modell abzubilden. Zusätzlich beschreibt das Modell noch mit Hilfe der beiden Relationen auf der rechten Seite, dass Entwicklungsartefakte entweder aus einem Prozess hervorgehen oder in diesen eingehen können. Links oben im Diagramm ist noch die Möglichkeit einer hierarchischen Strukturierung der Anforderungen modelliert.

Im unteren Diagramm sind die Zusammenhänge zwischen den einzelnen Entwicklungsartefakten beschrieben. Wie für die Anforderungen ist auch hier für Use Case, Prozess/Vorgehen und Tool, die Möglichkeit einer hierarchischen Strukturierung modelliert. Für Prozess/Vorgehen ist zusätzlich die Möglichkeit einer Prozesskette vorgesehen. Sämtliche weiteren Relationen beschreiben die Zusammenhänge zwischen den einzelnen Entwicklungsartefakten. Die Relationen sind dabei jeweils in Pfeilrichtung zu lesen. So ergibt sich z.B. für Schnittstelle der folgende Zusammenhang: Eine „Schnittstelle“ „basiert auf“ einem „Standard“. Die im oberen Diagramm beschriebenen Zusammenhänge sind weiterhin gültig. Dies lässt sich z.B. an Prozess/Vorgehen verdeutlichen. Im Kasten „references“ ist die Beziehung zu den Anforderungen abgebildet, obwohl das Diagramm selbst keinen Block mit Anforderungen enthält.

Die konkrete Dokumentation und Auswertung der Workshopergebnisse erfolgt durch die Instanziierung des Metamodells. Dazu werden die im Metamodell jeweils generalisiert beschriebenen Blöcke durch die realen Entwicklungsartefakte und Anforderungen der einzelnen Partner jeweils partnerspezifisch instanziiert. Die im Metamodell beschriebenen Relationen stellen die vordefinierten Zusammenhänge zwischen den einzelnen Instanzen her. Die Auswertung wird anschließend ebenfalls im Cameo-Systems-Modeller auf Basis der Instanzbildung durchgeführt.

Als Vorbereitung für die konkrete Durchführung der VVMethoden-Industrieworkshops wurde zudem zusammen mit dem TPX ein Fragenkatalog aus den Bereitstellungen der Teilprojekte erstellt. Dieser diente unter anderem dazu, es durch die gestellten Fragen den Industriepartnern zu erleichtern wichtige interne Stakeholder, die nicht direkt am Projekt beteiligt sind, inhaltlich abzuholen. Dies sollte den Industriepartnern eine fokussierte Vorbereitung auf die Workshops ermöglichen und durch diese Vorbereitung und Kenntnis der Inhalte, gegebenenfalls Stakeholder zu identifizieren die noch nicht direkt im Fokus waren. Die Rückläufer wurden zudem konsolidiert und vorab zur Schärfung und als Aufsatzpunkt der in den Workshop verwendeten Fragen verwendet. Abbildung 257 zeigt einen Ausschnitt aus dem mit TPX erarbeiteten Fragenkatalog.



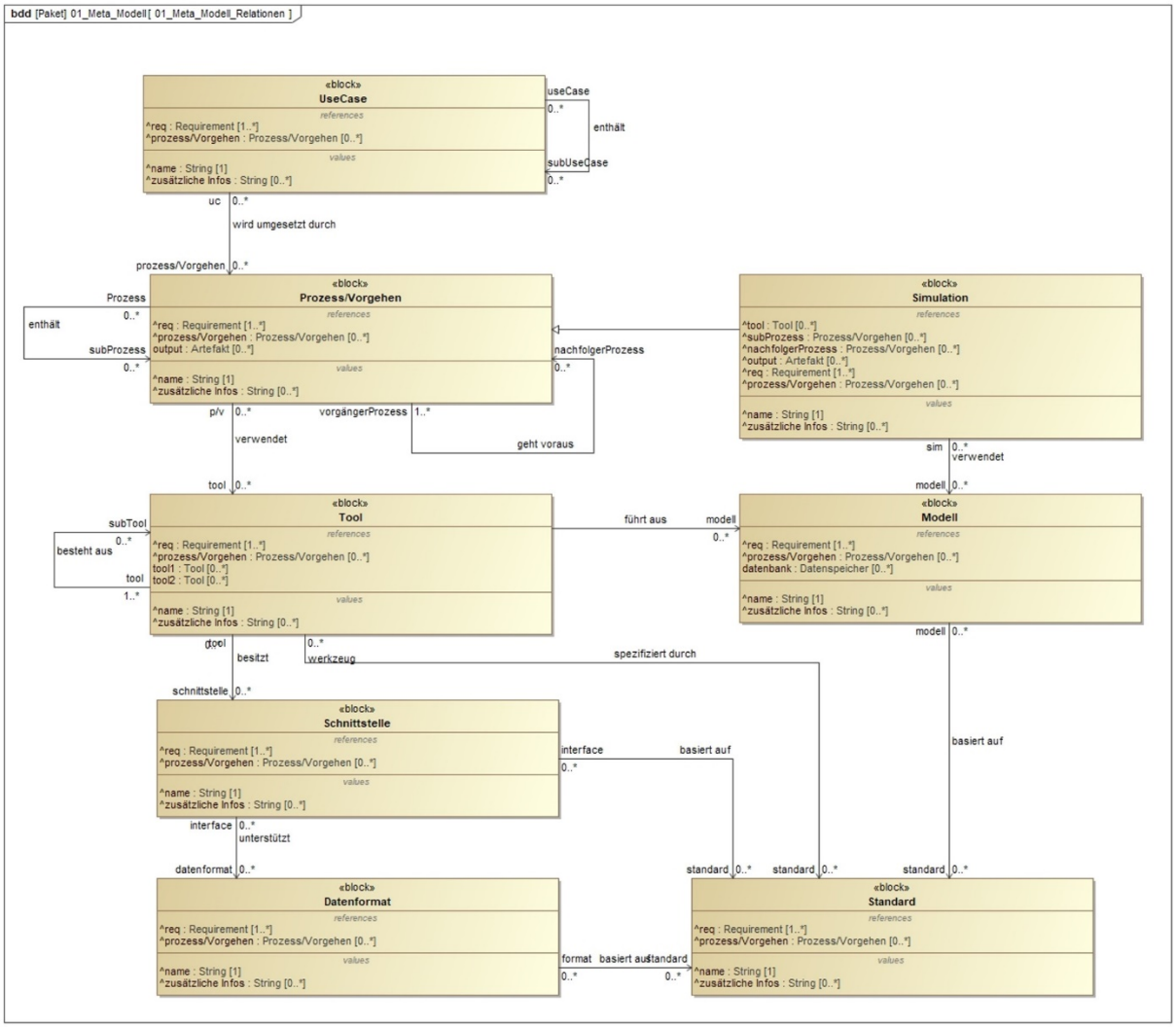


Abbildung 256: Metamodell in SysML zur Dokumentation und Workshopauswertung.

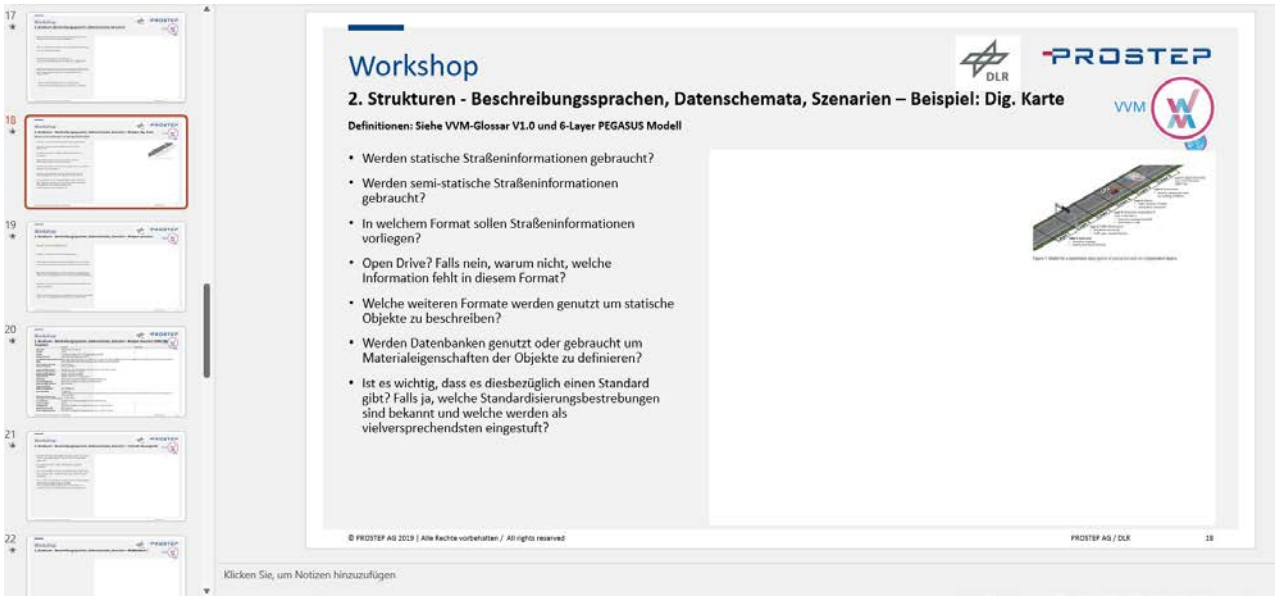


Abbildung 257: Ausschnitt aus dem mit TPX erarbeiteten Fragenkatalog.

Workshopdurchführung und Auswertung

Aufgrund des Ausbruchs der Corona-Pandemie 2020, konnte die Planung der jeweiligen Termine vor Ort für die gemeinsamen Industrieworkshops in der ursprünglichen Form nicht eingehalten werden. Geplant war hierbei, dass Mitarbeiter von PROSTEP zu den entsprechenden Partnern fahren und in Workshops vor Ort die Anforderungen aufnehmen, sowie den IST-Stand bei den Unternehmen gemeinsam erarbeiten. Wegen des Fortschreitens der Pandemie konnte lediglich ein Industrieworkshop in der zuvor angedachten Form Anfang 2020 durchgeführt werden.

Zur Durchführung des Vor-Ort-Workshops wurden seitens des Partners, zusätzlich zu den aus dem Teilprojekt 9 heraus eingeladenen Personen, jeweils Experten aus den verschiedenen Fachbereichen und Entwicklungsabteilungen identifiziert, die entsprechende Erfahrungen bei der Entwicklung von Komponenten und Funktionen für Fahrerassistenzsysteme und Systeme zum automatisierten und autonomen Fahren besitzen und zum Workshop mit eingeladen. Dies unterstützte einerseits die firmeninterne Sichtbarkeit des VVM-Projektes, andererseits konnte so auch über die Projektgrenzen hinaus vorhandenes, unternehmensspezifisches Expertenwissen mit einfließen.

Im Rahmen des Workshops konnten, wie oben beschrieben, der aktuelle IST-Zustand sowie der angestrebte SOLL-Zustand in Bezug auf VVMethoden relevante Themengebiete erarbeitet werden. Die auf diesem Wege erarbeiteten Inhalte wurden anschließend von PROSTEP aufbereitet und dem Partner zur Freigabe übermittelt. Nach erfolgter Freigabe flossen die Inhalte, bezüglich der Anforderungen und des IST-Zustandes, wie oben beschrieben, für die spätere Auswertung in das für diesen Zweck definierte SysML-Datenmodell im Cameo Systems Modeller ein. Abbildung 258 zeigt die Aufnahme einiger der Ergebnisse während des Vor-Ort-Industrieworkshop. Die eigentlichen Inhalte sind aus Vertraulichkeitsgründen unkenntlich gemacht.

Sämtliche weiteren Industrieworkshops im Rahmen des Teilprojektes 9 konnten anschließend nur noch im Online-Format durchgeführt werden. Insgesamt konnten mit neun Partnern Workshops durchgeführt werden.

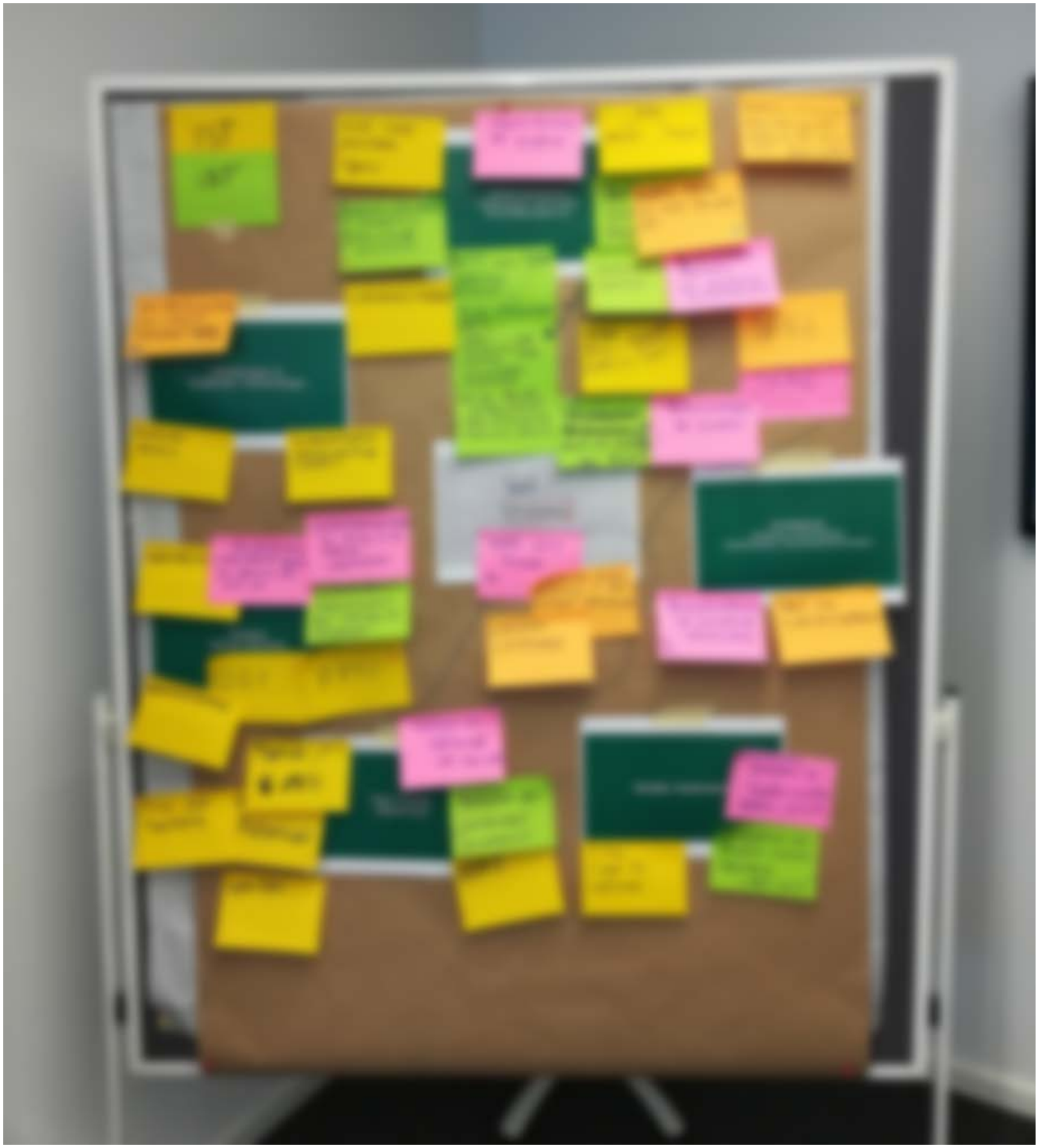


Abbildung 258: Teile des Ergebnisses des Vor-Ort-Workshops (aus Vertraulichkeitsgründen unkenntlich gemacht).

Wie oben angesprochen zeichnete sich im Laufe des Jahres 2020 immer mehr ab, dass die geplanten physischen Treffen mit den Industriepartnern vermutlich auf längere Zeit nicht durchführbar sind. Aus diesem Grund wurde frühzeitig eine Methode entwickelt, mit der die gemeinsamen Industrieworkshops online und toolgestützt durchgeführt werden können, um den Projektpartner die Möglichkeit zu geben, trotz coronabedingter Einschränkungen ihre Anforderungen an das Projekt zeitnah einzubringen.

Hierzu wurde das eingangs beschriebene, in SysML erarbeitete Metamodell, angepasst. Ziel der Anpassung war, das ursprünglich zur Auswertung und Aufbereitung der Workshopergebnisse

einzusetzende Modell, dahingehend abzuändern, dass es direkt in den Workshops verwendet werden kann. Dazu wurde das Modell zusätzlich in das Onlinetool Miro überführt, da aus lizenzrechtlichen Gründen eine gemeinsame Zusammenarbeit im SysML-Tool (Cameo Systems Modeller) nicht möglich war. Die Vorteile dieses Vorgehens bestehen somit, neben der zeitnahen Durchführung der Workshop darin, dass die Partner direkt vom Modell geleitet, zielgerichtet ihre jeweiligen Anforderungen einbringen können und eventuell noch bestehende Schwachstellen am Modell direkt in den Workshops identifiziert werden können.

Das Onlinekollaborationstool Miro wurde darüber hinaus bis Projektende, den Projektpartnern von PROSTEP zur Verfügung gestellt. Es kam dabei in verschiedensten Workshops und Meetings zum Einsatz, von Arbeitsgruppentreffen über Teilprojekttreffen bis hin zu Quartalstreffen und Gesamtprojektmeetings. Die in Miro dokumentierten Ergebnisse wurde bei Projektende von PROSTEP, soweit nötig exportiert und über das EICT allen Projektpartnern nachhaltig zur Verfügung gestellt.

Das Miro-basierte Format wurde für alle Online-Industrieworkshops einheitlich, mit jeweils einem Expertenteam aus verschiedenen Unternehmensbereichen des Partners, angewendet. Für die Überführung in Miro stellen die Elemente aus dem in Abbildung 256 dargestellten SysML-Diagrammen weiterhin die Basis dar. Die Zusammenhänge bzw. Relationen wurden weitestgehend übernommen und in Normalsprache ausgedrückt. Dazu waren jedoch an verschiedenen Stellen Anpassungen notwendig, da dabei auf Vererbungen verzichtet wurde, um dem Nutzer einen möglichst einfachen Einstieg zu ermöglichen. Für den Anwender stand somit in Miro ein ähnliches Metamodell, wie das in Abbildung 256 dargestellte zur Verfügung, wobei gleichzeitig die spätere Überführung der Ergebnisse in das SysML-Modell nicht beeinträchtigt wurde.

Da dem Modell in Miro keine standardisierte Modellierungssprache zugrunde liegt, wird der Anwender durch das Metamodell „nur geleitet“. Dies ermöglicht es ihm auch Zusammenhänge zu beschreiben, die im eigentlichen Modell nicht zulässig sind, bzw. Firmenspezifika einzubringen, die im SysML-Modell aufgrund der späteren Neutralisierung nicht abgebildet werden. Somit unterstützt dieses Vorgehen auch die Kommunikation der Ergebnisse ins Unternehmen und deren Akzeptanz, da bestimmte Sachverhalte, die für die spätere unternehmensinterne Weiterarbeit mit den Ergebnissen relevant sind, direkt miterfasst werden können. Und trotzdem wird der Anwender durch das geleitete modellbasierte Vorgehen nahe am Metamodell gehalten, um die Vergleichbarkeit mit anderen Projektpartnern sicherzustellen.

Abbildung 259 zeigt exemplarisch Ergebnisse verschiedener Online-Workshops. Die konkreten Inhalte sind aus Vertraulichkeitsgründen unkenntlich gemacht. In den Workshops konnten mit den Industriepartnern trotz der Coroan-Einschränkungen ihre Anforderungen, sowie ihr aktueller IST-Stand bezüglich angewendeter Methoden und (Simulations-)Prozesse, sowie eingesetzter Werkzeuge, Schnittstellen, Datenformate und relevanter Standards.

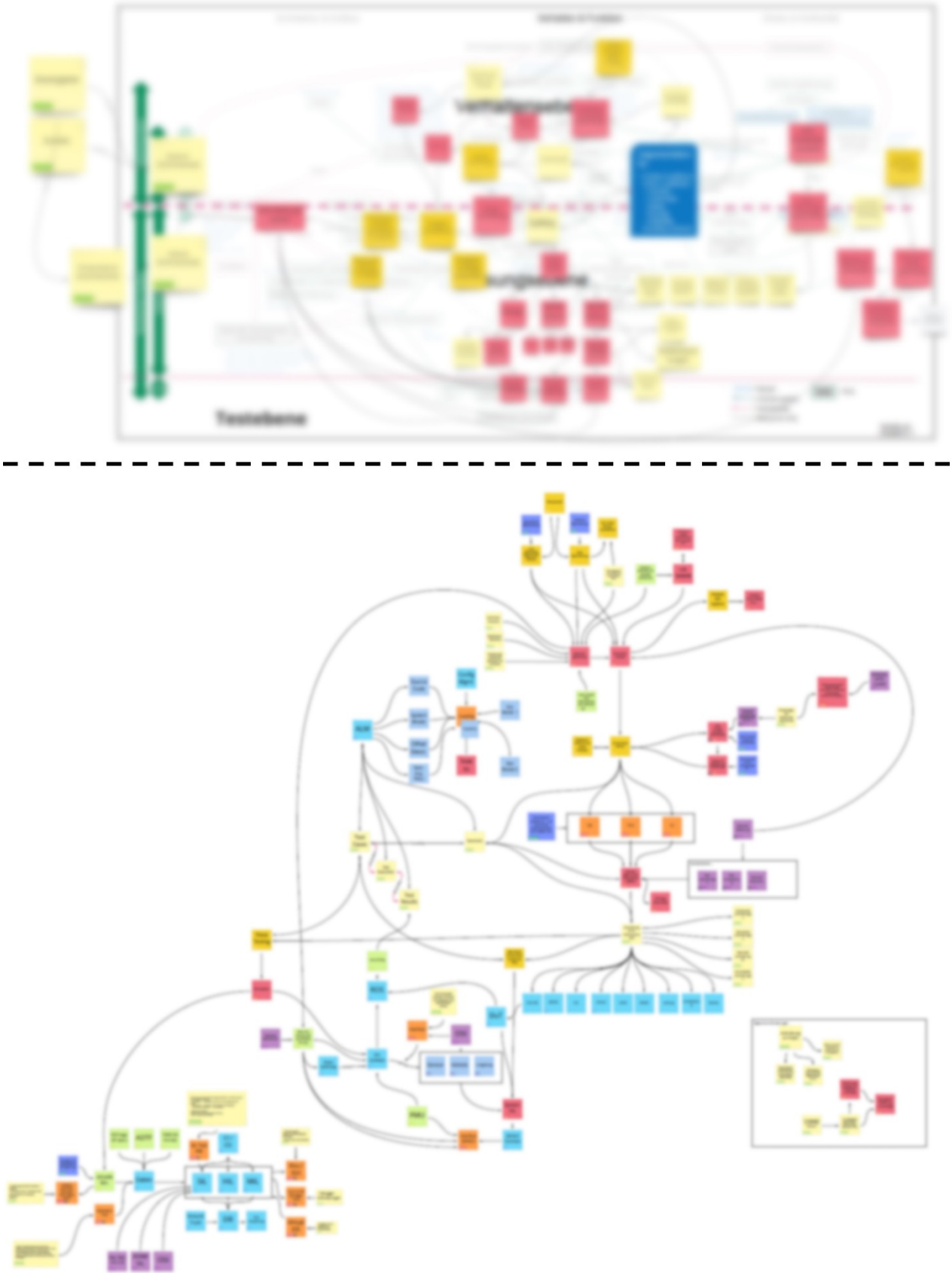


Abbildung 259: Exemplarische Ergebnisse verschiedener Online-Workshops (aus Vertraulichkeits-gründen unkenntlich gemacht),

Die in den (Online-)Workshops aufgenommenen Ergebnisse wurden partnerspezifisch dokumentiert. Dazu wurde zuerst, dass zusammen mit dem jeweiligen Partner erarbeitete Miro-Modell strukturiert, konsolidiert und die dokumentieren Artefakte jeweils partnerspezifisch neutralisiert. Die geschah zum Beispiel durch Entfernung von Produkt- oder Projektnamen aus den Inhalten, die einen direkten Rückschluss auf den jeweils beteiligten Partner zulassen.

Das auf diesem Weg überarbeitete Modell wurde anschließend an die jeweiligen Partner zur projektweiten Freigabe weitergeleitet. Auf Basis dieser Dem betreffenden Partner steht somit zusätzlich die überarbeitete „Rohversion“, für die firmeninterne Weiterarbeit zur Verfügung, die gegebenenfalls auch Inhalte enthalten kann, die nicht für das Gesamtprojekt gedacht oder als vertraulich eingestuft sind. Dies ermöglichte in den Workshops auch Inhalte zu diskutieren, die firmenintern und nicht für das Gesamtprojekt bestimmt waren, wodurch auch der firmeninterne Austausch unter den Beteiligten über die Abteilungsgrenzen hinweg gefördert werden kann.

Auf Basis der Rückmeldungen zur partnerspezifischen Freigabe wurden, soweit von Partnern gewünscht, Inhalte aus dem Miro-Modell entfernt, geschwärzt oder weiter neutralisiert. Aufbauend auf diesen Rückläufern flossen die freigegebenen Inhalte in das partnerübergreifende SysML-Modell in der neutralisierten Version ein.

Dieses Vorgehen ermöglichte die anonymisierte Auswertung und Bereitstellung der Ergebnisse im Projekt. Die Gesamtheit, der auf diesem Wege mit den Partnern erarbeiteten Inhalte, wurde themenspezifisch kategorisiert, für die partnerübergreifende Priorisierung ausgeleitet und an die Partner übergeben. Für die Priorisierung der Anforderungen wurden diese, zur leichteren Auswertbarkeit, in verschiedene Kategorien, basierend auf den Themengebieten der gesammelten Anforderungen, eingeteilt. Die Auswertung der Priorisierung fand anhand dieser Themencluster statt. Abbildung 260 zeigt die für die Priorisierung identifizierten und verwendeten Themencluster der Anforderungen.

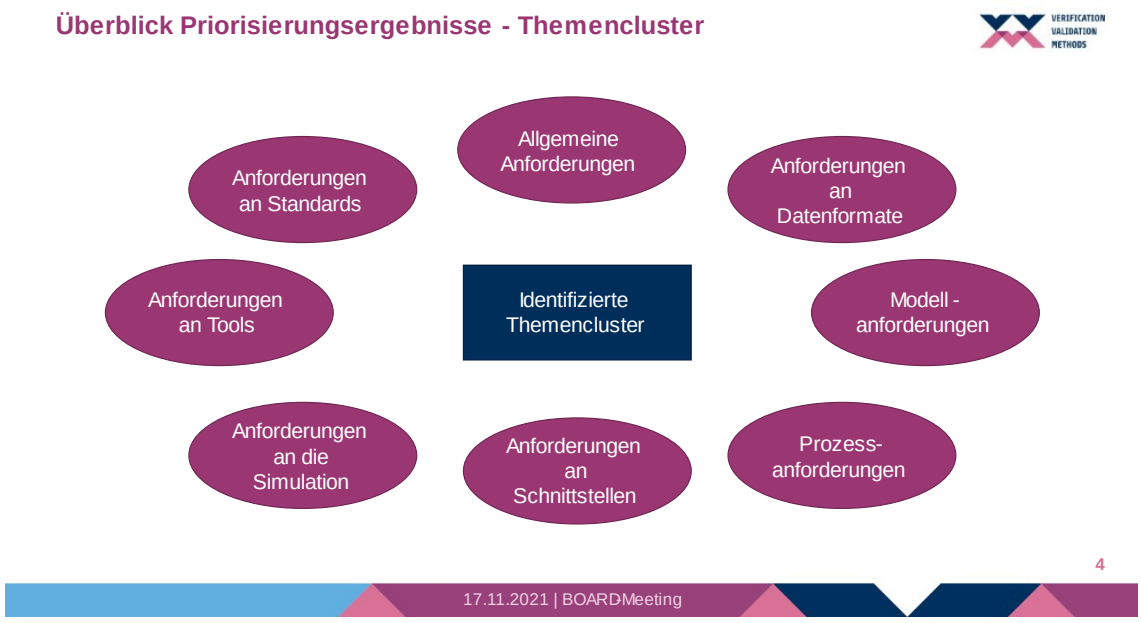


Abbildung 260: Überblick der Themencluster für die Priorisierung.

Für die themenspezifische Kategorisierung der Anforderungen, wurde diese zuerst, auf Basis der erarbeiteten Inhalte, als konkrete Anforderungen in Form einer Anforderungsaussage formuliert

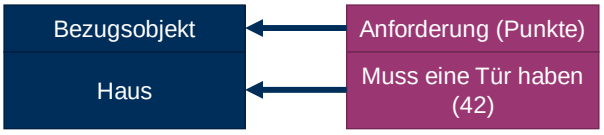
(vgl. „Der Abschlussbericht von VVM muss veröffentlicht werden.“). Dies geschah aus dem Grund, dass viele der Anforderungen im Miro-Modell als SOLL-Zustand bzw. in der Notation „Objekt erfüllt Requirement“ (vgl. Abbildung 256) erfasst wurden, aber nicht in einer formalen Schreibweise für Anforderungen. Zusätzlich wurde für die Übergabe der Anforderungen an die Partner zur Priorisierung, jede Anforderung mit ihrem im Modell zugehörigen Bezugsobjekt verknüpft. Dies geschah einerseits aus dem Grund, dass sich teilweise Anforderungen auf mehrere Objekte und damit auch Anforderungskategorien bezogen. Andererseits erleichtert die genaue Zuordnung den Partnern, dass Verständnis der Anforderung.

Ein Großteil der zu bewertenden Anforderungen wurde von anderen Partnern eingebracht. Damit ist es essenziell die Anforderungen so abzubilden, dass die Beschreibung selbsterklärend ist und möglichst wenig Interpretationsspielraum zulässt. Abbildung 261 zeigt einen Überblick über das Priorisierungsschema der Anforderungen, dass den Partner vorgestellt wurde. Für die Bewertung durch die Partner kann eine Punktevergabe nach Relevanz der Anforderungen vorgenommen werden (vgl. Abbildung 261 oben). In der Abbildung unten, ist das Zuordnungsschema für eine exemplarische Anforderung dargestellt.

Basierend auf den Rückmeldungen der Partner wurden die Ergebnisse der Priorisierung der Anforderungen im Anschluss wieder partnerübergreifend zusammengeführt, um auch hier eine Anonymisierung der Ergebnisse sicherzustellen und keine Rückschlüsse auf die jeweilige Priorisierung durch die Partner zu ermöglichen.

Priorisierungskategorien	Punkte
Wird als essentiell angesehen	9
Wird als sehr relevant angesehen	3
Wird als relevant angesehen	1

Vorstellung der Anforderungen die im Schnitt von mindestens einem Partner als essentiell angesehen werden



Vorstellung der Anforderungen grundsätzlich mit dem jeweiligen Bezugsobjekt

Abbildung 261: Vorgehen zur Darstellung der zu priorisierenden Anforderungen.

Im Rahmen der gesamten VVM-Industrieworkshops konnten über 150 Anforderungen zusammen mit den VVM-Industriepartnern erarbeitet und anschließend priorisiert werden.

Die Ergebnisse der Priorisierung sind im Rahmen eines BOARD-Meetings (vgl. hierzu Kapitel 3.1.2.9.4.2 „Results-Board und Ergebnisverbreitungsprozess (Projektinternes Baselining)“) an das Projekt kommuniziert und übergeben worden. Dabei wurden alle Anforderungen betrachtet, die

von mindestens einem Partner als essenziell angesehen werden (vgl. Abbildung 261 oben) und daraus Kernbotschaften für das Projekt abgeleitet:

- Einheitliche **Schnittstellen** und **Austauschformate**, sowie ein **standardisierter** Modellaustausch sind zu forcieren
- Die **Qualität** von eingesetzten Tools und verwendeten Simulationen muss **prüfbar** und **validierbar** sein
- **Industrialisierung** einer **standardisierten Zulassungsfähigkeit** eines automatisierten Fahrzeugs unter Berücksichtigung **rechtlicher Randbedingungen** und **Sicherheitsanforderungen** (Sicherheitsargumentation) sowie der Sicherstellung der **Sicherheit der Fahrzeuge** zum und nach dem Auslieferungszeitpunkt
- **Kritikalitätsanalyse** wird als ein zentraler Aspekt der Sicherheitsargumentation angesehen
- Sicherstellen der **Durchgängigkeit** und **Traceability** werden als elementarer Teil der Absicherungskette angesehen
- **Umfang** und **Limitation** des Einsatzes von **Simulationen** für die Absicherung

Die gesammelten Erkenntnisse wurden hierzu abschließend im VVM-Confluence, inklusive der Präsentation zum BOARD-Meeting, abgelegt und stehen dem Gesamtprojekt zur Verfügung. Sämtliche Anforderungen sind dazu inklusive deren Priorisierung im Confluence abgelegt und damit dem Projekt zugänglich gemacht worden. Darüber hinaus ist ebenfalls der zum Zeitpunkt der Erhebung aufgenommene IST-Zustand im Confluence partnerübergreifend und neutralisiert abgelegt.

Austausch mit TPX

Im Anschluss an die zuvor beschriebene Anforderungserhebung und Priorisierung der Anforderungen wurde ein weiterer optional anzuwendender Prozessvorschlag für die im Projekt freigegeben und anonymisierten Anforderungen erarbeitet.

Abbildung 262 stellt schematisch den Prozessvorschlag zur Übergabe für das TPX relevanter Inhalte an dieses dar. Die Farben stellen dabei zur besseren Unterscheidung die jeweiligen beteiligten Projektinstanzen in Lila und Grün (VVMethoden, und TPX) dar. Zusätzlich ist in Blau die Untermenge der priorisierten Anforderungen und der für VVMethoden relevanten WG13-Inhalte dargestellt. Die Zahlen geben jeweils die Zeitpunkte bzw. die Reihenfolge der Prozessschritte an. Die Arbeiten der WG13 sowie die Anforderungserhebung und Priorisierung im VVM-Projekt erfolgen zeitlich parallel und unabhängig voneinander (1). Durch seine Arbeit in der WG13 ermittelt das TPX, Inhalte und Themen für die, die Ergebnisse der Anforderungserhebung relevant sein könnten (2). Für die WG13 relevante Inhalte sollen nach Rücksprache mit den Partnern gegebenenfalls an die WG13 übergeben werden (3 und 4). Dies hat die Ziele industrierelevante Anforderungen aus dem VVMethoden-Projekt in die WG13 zu tragen und im Gegenzug Feedback zu den Industrieanforderungen aus der WG13 zu erhalten (5). Dieses Feedback sowie die Anforderungen selbst können zu jedem Zeitpunkt an das VVM-Projekt übergeben werden.

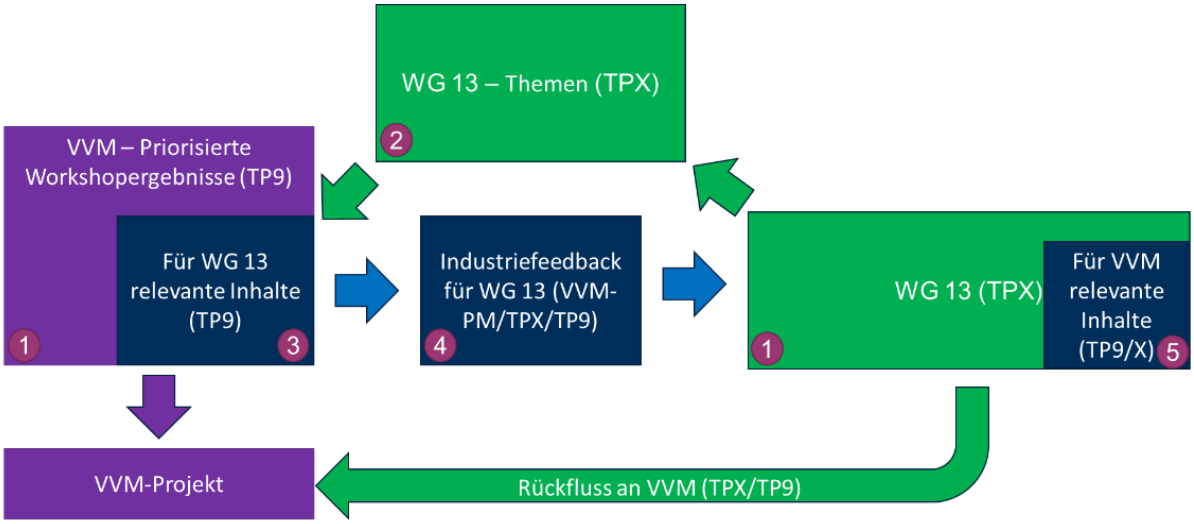


Abbildung 262: Prozessvorschlag für den Austausch mit der WG13 über das TPX und TP9.

Unabhängig davon wurde die Sammlung der während des Anforderungserhebungsprozesses identifizierten Standards nach Freigabe durch das Projekt und Anonymisierung an das TPX zur weiteren Verwendung übergeben.

3.1.2.9.3 Unterstützung für die Instanziierung

In der Industrie ist heute ein Trend hin zur Digitalisierung und Virtualisierung von Produktentwicklungsprozessen zu beobachten. Die Entwicklung von technischen Systemen betrifft viele verschiedene Domänen und Unternehmensbereiche. Dies gilt insbesondere für die Entwicklung von automatisiert fahrenden Fahrzeugen, aber auch für die meisten anderen komplexen technischen Entwicklungen. Die Kenntnis aller Artefakte und ihrer Zusammenhänge und Abhängigkeiten, insbesondere über Domänengrenzen hinweg, ist entscheidend für einen konsistenten Entwicklungsprozess und unterstützt den Umgang mit Komplexität. Um die Konsistenz zu gewährleisten, ist einer der wichtigsten Ansätze im VVMethoden-Projekt die Verwendung der Assurance-Argumentation zum Nachweis der Konformität und gleichzeitig als strukturierender Ansatz zur Beherrschung der Komplexität.

In den letzten Jahren war das hochautomatisierte Fahren weltweit ein Bestandteil einer Vielzahl von Forschungsinitiativen, zu denen auch das VVMethoden-Projekt zählt. Auf nationaler Ebene wären hier neben anderen beispielsweise das PEGASUS-Projekt, sowie das eng mit VVMethoden verbundene Schwesterprojekt SET Level zu nennen.

Die Erwartungen, die an das hochautomatisierte Fahren gestellt werden reichen dabei, beispielsweise von einer Steigerung der Verkehrseffizienz über die Erhöhung der Verkehrssicherheit bis hin zur Emissionsreduktion [114].

Wie eingangs geschrieben sind hochautomatisierte Straßenfahrzeuge als komplexe Systeme anzusehen. Zusätzlich zu den oben beschriebenen Herausforderungen, die sich daraus ergeben, sollen diese Fahrzeuge jedoch zusätzlich in einem hochkomplexen Umfeld, bespielweise im innerstädtischen Verkehr, betrieben werden. Generell zeichnet sich ein Trend dahingehend ab, dass Simulationen immer mehr Einzug in die Entwicklung und auch die Absicherung von Systemen erhalten. Virtuelle Prototypen beziehungsweise Simulationsmodelle kommen dabei

neben der Auslegung der Systeme auch vermehrt zur Absicherung sicherheitsrelevanter Systeme oder Systemaspekte zur Anwendung [115].

Im Falle des hochautomatisierten Fahrens erscheint eine reine Validierung z.B. durch reale Versuchsfahrten oder Tests als nicht gangbar. Eine virtuelle Absicherung bietet hierbei unter anderen sicher die Vorteile, dass bestimmte Umgebungseffekte, Umweltbedingungen oder Fehlfunktionen sicherer und effizienter untersucht werden können als dies mit realen Versuchsträgern der Fall ist. Darüber hinaus kann eine virtuelle Absicherung aber zum Beispiel auch zwingend notwendig werden, wenn die für die Absicherung notwendige Versuchskilometer mit realen Prototypen nicht mit vertretbarem Aufwand aufgenommen werden können [44]. Auch können rechtliche Randbedingungen existieren, die es nötig machen ein System virtuell abzusichern, bevor es in einen realen Einsatz kommen darf, da bestimmte Fehlerfälle oder Randbedingungen mit realen Prototyen nicht sicher oder effizient durchzuführen sind.

Für die Schaffung von Test und Absicherungsverfahren ist dabei nicht nur nötig diese technisch umsetzbar zu gestalten. Ein elementarer Aspekt innerhalb der Verifikation und Validierung von hochautomatisierten Fahrzeugen, ist es auch das zugrundeliegende Verfahren bzw. die Methode nachvollziehbar und durchgängig zu gestalten sowie das Vertrauen von seitens Dritter in die Methode sicherzustellen.

Das VVMethoden-Projekt hat dazu eine Gesamtmethode entworfen, die einerseits bereits früh im Entwicklungsprozess bei der Definition von Anforderungen und Sicherheitskonzepten startet, um wesentliche Sicherheitsaspekte des hochautomatisierten Fahrzeugs bereits frühzeitig konstruktiv berücksichtigt zu können. Zudem werden auch Aspekte wie Risikobetrachtung, Szenarienerstellung, Kundenfunktionen und das produzierende Unternehmen mit einbezogen. Damit wird die Möglichkeit geschaffen, basierend auf den einzelnen Methodenbausteinen eine nachvollziehbare und glaubwürdige Sicherheitsargumentation durchzuführen. Abbildung 263 zeigt die Hauptelemente der initialen Darstellung der Methodenzusammenführung der VVM-Methode.

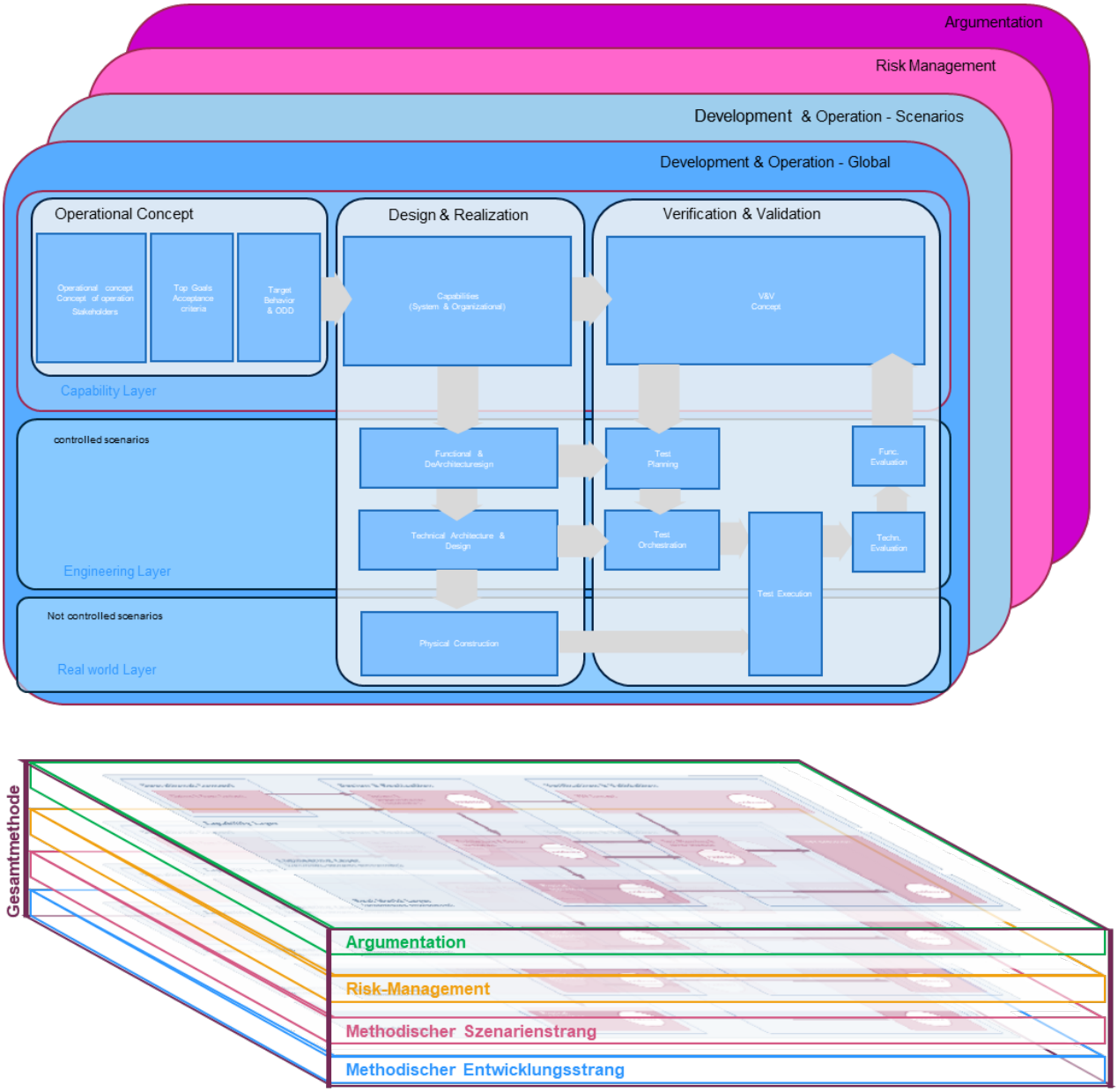


Abbildung 263: VVM-Gesamtmethode – Methodenzusammenführung initiale Darstellung.

Dazu hat PROSTEP die im VVMethoden-Projekt erstellten Methodenbausteine gesamtheitlich in einem SysML-Modell zusammengeführt. Ebenso wurde die Gesamtmethode auf Basis des im Projekt entwickelten Traceability Demonstrator, implementiert. Ziel war dabei unter anderem, eine Unterstützung für die spätere Einführung bzw. Adaption der im Projekt erarbeiteten Prozesse und Methoden in den Unternehmen zu schaffen.

Dazu wurde eine Vielzahl von Workshops moderiert, um zusammen mit den Forschungspartnern und den Industriepartnern die Grundlage für eine möglichst reibungsfreie Einführung der VVMethoden-Ergebnisse in den Unternehmen zu gewährleisten und einen Rückfluss in die industrielle Anwendung sicherzustellen. Die Dokumentation der Methode ist dabei so gestaltet, dass die Projektpartner selbständig entscheiden können, ob sie die kompletten Prozesse und Methoden einsetzen wollen, oder gegebenenfalls nur Teilaspekte umsetzen.

Die Dokumentation der Gesamtmethode besteht aus zwei Hauptfeldern. Zum einen die Beschreibung des in SysML erstellten Modells der VVM-Gesamtmethode (Kapitel 3.1.2.9.4) und zum anderen aus der Darstellung der Umsetzung der Inhalte der Gesamtmethode im, im Projekt von PROSTEP entwickelten Traceability Demonstrator TRACY (Kapitel 3.1.2.9.5). PROSTEP leistet damit einen Beitrag zur industriellen Instanziierbarkeit der Projektergebnisse und zur späteren Dissemination über das Projekt hinaus.

Im Folgenden sind einige der Hauptnutzungspotentiale für und Vorteile durch die Anwendung der Modellierung und Implementierung aufgeführt:

- Globale Struktur nach den vier **„Hauptbausteinen"** der **VVM-Methode.**
- Grafische Darstellung unterstützt den einfachen Zugang zur **VVM-Methode.**
- Das SysML-Modell unterstützt das allgemeine Verständnis der **Zusammenhänge** zwischen den Prozessschritten (Aktivitäten) sowie der zwischen ihnen **ausgetauschten Artefakte**.
- Das SysML-Modell unterstützt die **Konsistenz** der VVM-Methode und der **Schnittstellen** zwischen den Prozessschritten.
- Die formalisierte Beschreibung der VVM-Methode erleichtert die **Diskussion** und **Koordination**.
- Der einfach zu bedienende **HTML-Export** des SysML-Modells unterstützt die Navigation durch die gesamte **VVM-Methode**
- Die aktuelle Implementierung der **VVM-Methode** in TRACY kann als **"Blaupause"** für die industrielle Anwendung genutzt werden.

3.1.2.9.4 Die Gesamtmethode im SysML-Modell

3.1.2.9.4.1 Vorarbeiten, Begründung und generelles Vorgehen

Die Dokumentation der Gesamtmethode soll die industrielle Instanziierbarkeit von Projektergebnissen unterstützen. Dazu wurde das im VVM-Projekt entworfene stakeholderorientierte Vorgehen zum Baselining im Engineering Prozess verwendet. Anhand des initialen confluncebasierten Vorgehens, in dem die Projektergebnisse basierend auf den Synchronisationspunkten der VVM-Methode gesammelt werden, wurden zahlreiche Einzelgespräche und Workshops mit den Verantwortlichen für die Synchronisationspunkte geführt.

Die dadurch identifizierten Schnittstellen zwischen den Synchronisationspunkten und deren Abgleich ermöglichen eine durchgängige Beschreibung der Methode, was die industrielle Anwendbarkeit und Instanziierung verbessert bzw. erst ermöglicht. Ziel des im Projekt abgestimmten Vorgehens ist es im Rahmen dessen, die Durchgängigkeit der Synchronisationspunkte des Assurance Frameworks sowie die Verknüpfung der Szenarien mit diesem sicherzustellen. Darüber hinaus wurde im Laufe des Vorgehens auch der Zusammenhang zur Argumentation und zum Risk Management mit integriert.

Die Schaffung einer durchgängigen und konsistenten Beschreibung der VVM-Methode unterstützt dabei auch die spätere Instanziierbarkeit in den Häusern. So können Methodenbausteine eindeutig in der Methode verortet werden und es werden auch deren Zusammenhänge mit anderen Methodenbausteinen ersichtlich. Dies ermöglicht es z.B. einzelne Inhalte der Methode in den

Häusern anzuwenden und in ein ggf. bereits bestehendes Vorgehen zu integrieren, da die Schnittstellen der Bausteine bzw. Synchronisationspunkte klar beschrieben sind.

3.1.2.9.4.2 Results-Board und Ergebnisverbreitungsprozess (Projektinternes Baselining)

Dieses Vorgehen wird zusätzlich durch den bereits früh im Projekt gemeinsam mit dem Teilprojekt 1 und PROSTEP im Teilprojekt 9 entwickelten Prozess zum projektinternen Baselining und der projektinternen Ergebnisfreigabe und Dokumentation unterstützt. Die Umsetzung des Prozesses im Rahmen von BOARD-Meetings wurde durch das EICT und die Projektpartner innerhalb der Projektlaufzeit zyklisch bis zum Projektende betrieben.

Abbildung 264 zeigt den initial von PROSTEP im Teilprojekt 9 entworfenen Prozess zum Aufbau einer Confluence-Seite zur Ergebnisverbreitung. Hierzu wird initial eine Confluence-Seite aufgesetzt, die im Laufe des Prozesses mit den jeweils für einen Review in Frage kommenden Ergebnissen befüllt wird. Zusätzlich werden dabei die Verantwortlichen für die jeweiligen Ergebnisse benannt und es können sich Projektpartner, die am Ergebnis interessiert sind, eintragen. Nach Fertigstellung des Ergebnisses werden diese informiert über den Termin der Vorstellung informiert, der zugehörige Link zum Ergebnis zur Verfügung gestellt und entschieden, ob das Ergebnis auch Relevanz für TPX hat. Das Vorgehen wurde mit allen Teilprojektleitern abgestimmt und eine Seite zur Dokumentation und Steuerung des Prozesses in Confluence zur Verwendung im Gesamtprojekt erstellt. Ein Ausschnitt dieser Seite ist in Abbildung 265 zu sehen. Hier wurde noch zusätzlich eine Spalte ergänzt, falls ein Steuerkreisbeschluss nötig ist.

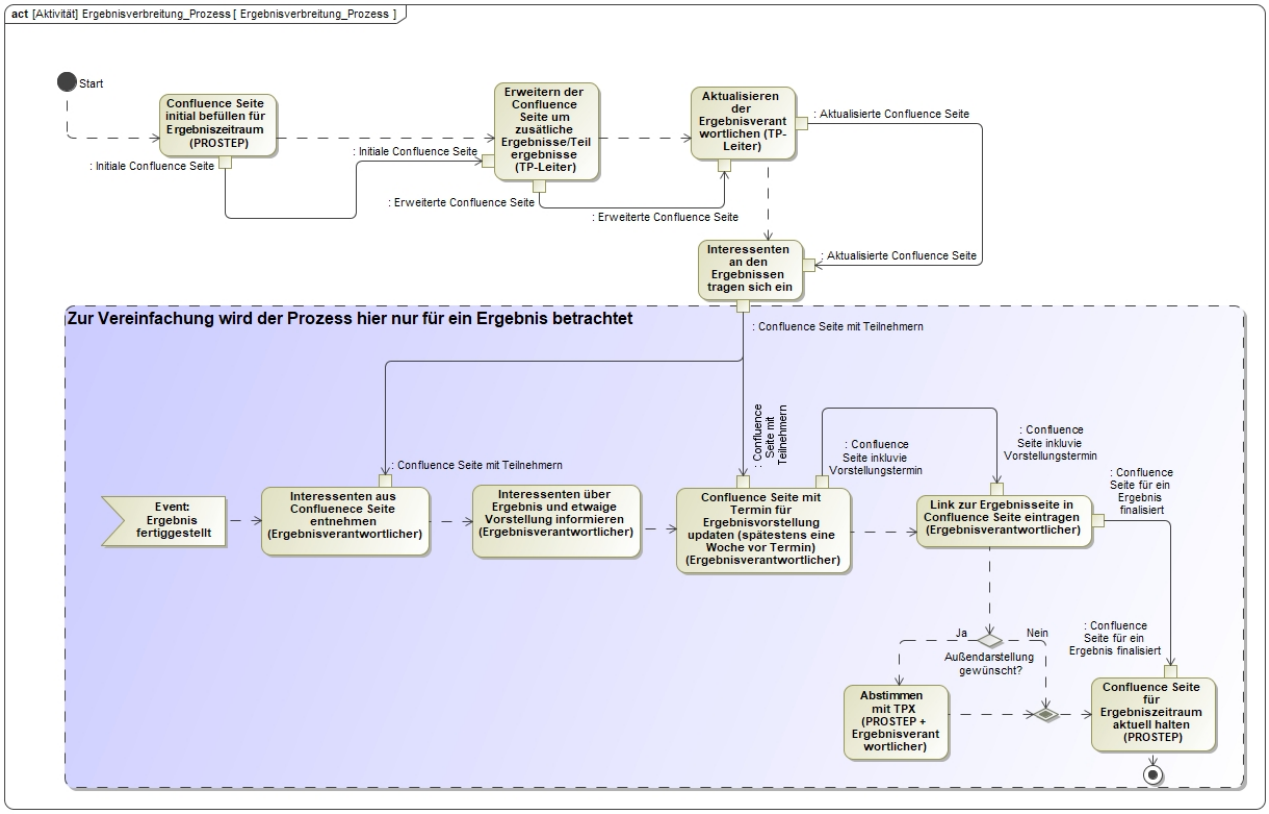
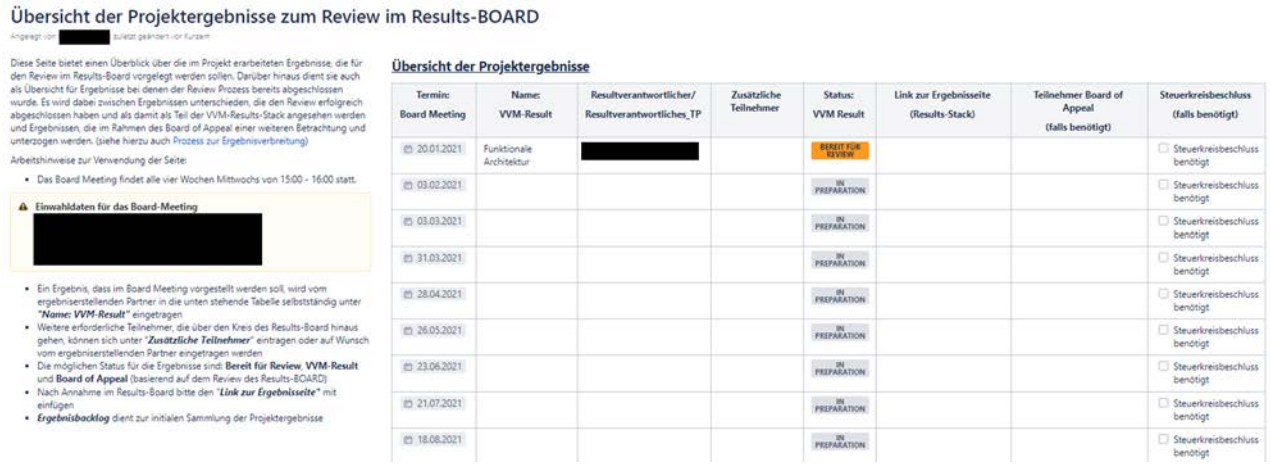


Abbildung 264: Initialer Prozessvorschlag zum Aufbau einer steuernden Confluence-Seite für den Ergebnisverbreitungsprozess.



Übersicht der Projektergebnisse zum Review im Results-BOARD

Angelegt von [redacted] zuletzt geändert vor Kurzem

Diese Seite bietet einen Überblick über die im Projekt erarbeiteten Ergebnisse, die für den Review im Results-Board vorgelegt werden sollen. Darüber hinaus dient sie auch als Übersicht für Ergebnisse bei denen der Review Prozess bereits abgeschlossen wurde. Es wird dabei zwischen Ergebnissen unterschieden, die den Review erfolgreich abgeschlossen haben und als damit als Teil der VVM-Results-Stack angesehen werden und Ergebnissen, die im Rahmen des Board of Appeal einer weiteren Betrachtung und unterzogen werden. (siehe hierzu auch Prozess zur Ergebnisverbreitung)

Arbeitshinweise zur Verwendung der Seite:

- Das Board Meeting findet alle vier Wochen Mittwochs von 15:00 - 16:00 statt.

⚠ Einwahldaten für das Board-Meeting

[redacted]

- Ein Ergebnis, dass im Board Meeting vorgestellt werden soll, wird vom ergebniserstellenden Partner in die unten stehende Tabelle selbstständig unter ***"Name: VVM-Result"*** eingetragen
- Weitere erforderliche Teilnehmer, die über den Kreis des Results-Board hinaus gehen, können sich unter ***"Zusätzliche Teilnehmer"*** eintragen oder auf Wunsch vom ergebniserstellenden Partner eingetragen werden
- Die möglichen Status für die Ergebnisse sind: **Bereit für Review**, **VVM-Result** und **Board of Appeal** (basierend auf dem Review des Results-BOARD)
- Nach Annahme im Results-Board bitte den ***"Link zur Ergebnisseite"*** mit einfügen
- ***Ergebnisbacklog*** dient zur initialen Sammlung der Projektergebnisse

Übersicht der Projektergebnisse

Termin: Board Meeting	Name: VVM-Result	Resultverantwortlicher/ Resultverantwortliches_TP	Zusätzliche Teilnehmer	Status: VVM Result	Link zur Ergebnisseite (Results-Stack)	Teilnehmer Board of Appeal (falls benötigt)	Steuerkreisbeschluss (falls benötigt)
20.01.2021	Funktionale Architektur	[redacted]		BEREIT FÜR REVIEW			Steuerkreisbeschluss benötigt
03.02.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
03.03.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
31.03.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
28.04.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
26.05.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
23.06.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
21.07.2021				IN PREPARATION			Steuerkreisbeschluss benötigt
18.08.2021				IN PREPARATION			Steuerkreisbeschluss benötigt

Abbildung 265: Genereller Aufbau der Confluence-Seite zur projektinternen Ergebnisfreigabe und Dokumentation (personenbezogene Inhalte geschwärzt).

Das konkrete, auf Basis der Confluence Seite durchgeführte, Vorgehen zu projektinternen Baselining gliedert sich dabei in verschiedene in Abbildung 266 dargestellte Schritte. Vorab wird entschieden, ob das jeweilige Ergebnis einen ausreichenden Reifegrad hat und ob ein erweiterter Kreis aufgrund der Relevanz als VVMethoden-Gesamtergebnis das Ergebnis begutachten soll. Sollte der Reifegrad nicht erfüllt sein, wird es zur weiteren Bearbeitung an die Verantwortlichen übergeben. Fällt die zweite Entscheidung negativ aus, verbliebt es als Teilprojektergebnis in der Verantwortung des jeweiligen TPs. Werden beide Vorabbegutachtung mit „Ja“ beantwortet, findet ein Review im Rahmen eines Board-Meetings statt. Bei erfolgreichem Durchlaufen wird es in den sogenannten „Resultsstack“ aufgenommen und kann ggf. zur weiteren Dissemination über das Projekt im Rahmen des TPX verwendet werden. Sollte der Review nicht erfolgreich durchlaufen werden und kein Konsens gefunden werden, wird das betreffende Ergebnis von der ergebniserzeugenden Partei, sowie der „ablehnenden“ Partei erneut überarbeitet. Die „ablehnende“ Partei unterstützt hierbei aktiv die Überarbeitung. In letzter Instanz würde, im sehr unwahrscheinlichen Fall, dass trotzdem kein Konsens gefunden wird, der Weg über den Steuerkreis gesucht werden.

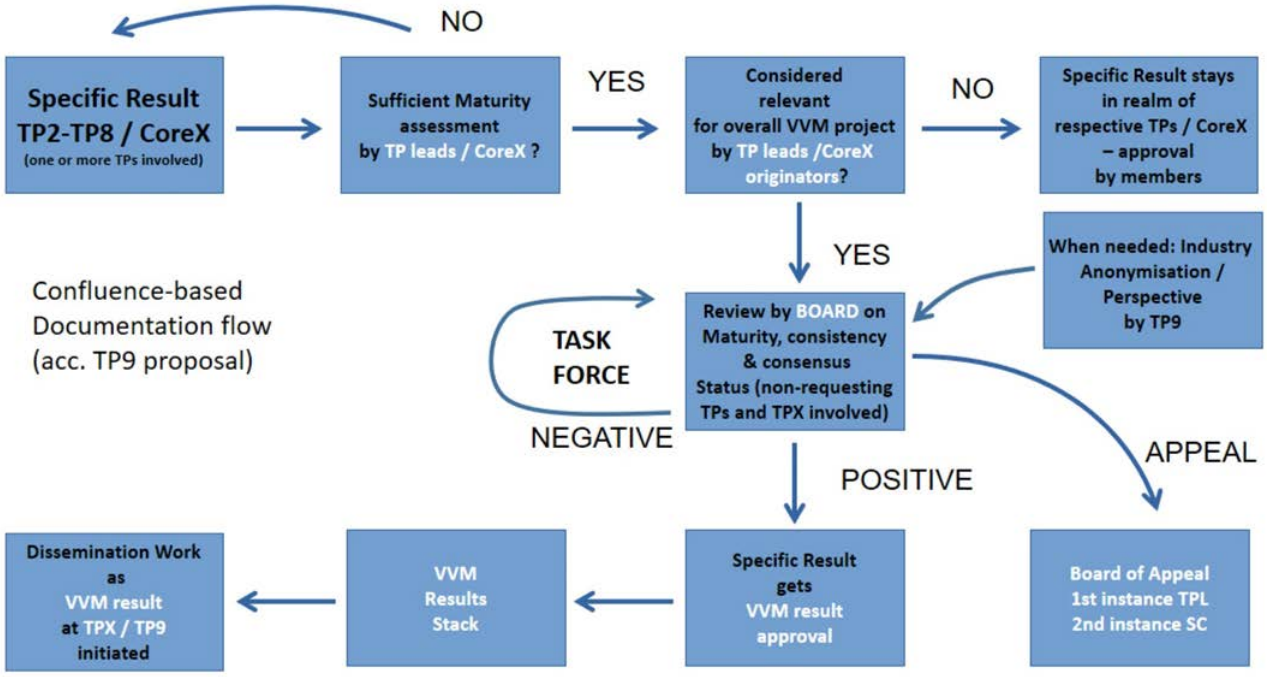


Abbildung 266: Ergebnisverbreitungsprozess (projektinternes Baselining).

3.1.2.9.4.3 Hinführung zum Baselining im Engineering Prozess

Als Vorüberlegung und zur Veranschaulichung des Vorgehens zur späteren Darstellung der VVM-Gesamtmethode als Prozess wurde die PEGASUS-Gesamtmethode [36] von PROSTEP in einer Prozesssicht dargestellt. Ziel war es das später umgesetzte Vorgehen zum Baselining im Engineering Prozess an einer den Projektpartnern und der Community bekannten Methode zu demonstrieren und zu verdeutlichen. Der Vorteil liegt zusätzlich darin, dass die verwendete PEGASUS-Methode [36] bereits vollständig beschrieben und etabliert war und sie somit unabhängig vom VVM-Projektfortschritt der einzelnen Bausteine der VVM-Gesamtmethode genutzt werden konnte. Wie im später angewendeten Vorgehen zum Baselining im Engineering Prozess wurden auch hier die einzelnen Schritte innerhalb der PEGASUS-Methode [36] als eine Reihe von aufeinander folgenden Aktivitäten dargestellt. Diese tauschen, wie in der späteren Darstellung der VVM-Gesamtmethode, ebenfalls Entwicklungsartefakte als Übergabeobjekte aus. Die initiale Darstellung der Überführung der PEGASUS-Methode [36] in einen Prozess mit In- und Outputs ist in Abbildung 267 dargestellt. Aufgrund der sich ergebenden Form wurde diese Darstellung auch als E-Gitarren-Darstellung bezeichnet.

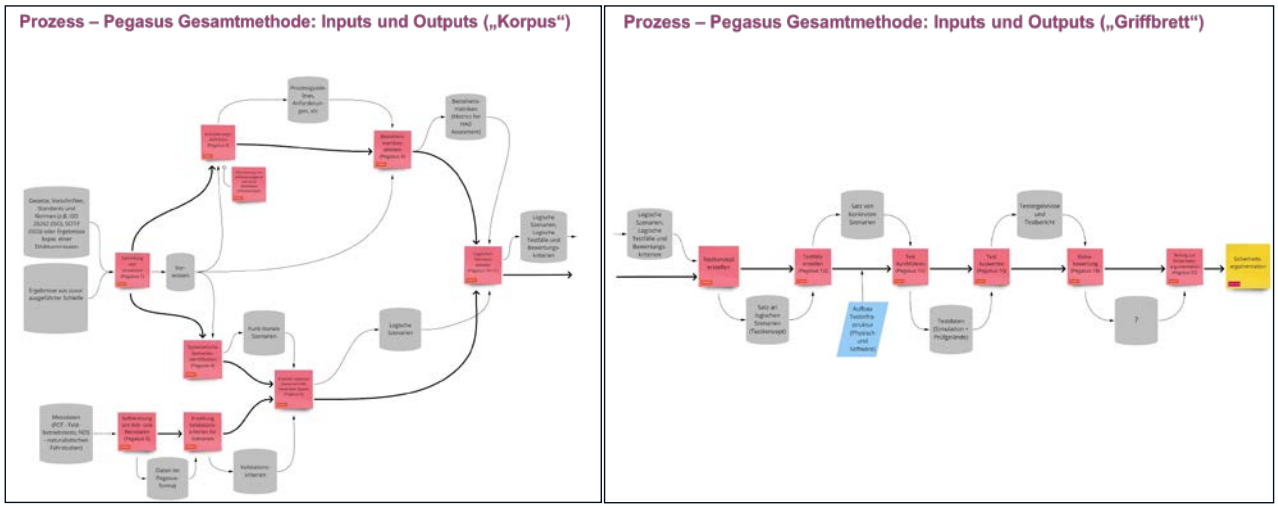


Abbildung 267: PEGASUS-Methode [36] als Prozessdarstellung mit In- und Outputs.

In der Darstellung wurden die jeweiligen Prozessschritte in Rot dargestellt und zur leichtern Zuordnung mit den zugehörigen Nummern der Elemente aus der PEGASUS-Gesamtmethode [36] versehen. Die Übergabeobjekte zwischen den einzelnen Prozessschritten sind in Grau dargestellt.

Im weiteren Verlauf wurde dieses Vorgehen auch erstmalig auf die zu diesem Zeitpunkt als Informationsfluss vorliegende Darstellung der VVM-Methode angewendet. Hierbei ist die gleiche Konvention zur Farbgebung und Darstellung wie zuvor für die Beschreibung der PEGASUS-Methode [36] zur Anwendung gekommen. Abbildung 268 zeigt oben, die im Projekt entwickelte Darstellung des Informationsflusses. Im selben Bild, unten, ist der davon abgeleitete Prozessfluss mit den einzelnen Aktivitäten und den zugehörigen In- und Outputs dargestellt. Hierbei wird explizit wie oben im Bild auch, durch die farbigen Rahmen dargestellt, zwischen einem sensorbezogenen und einem szenarienbezogenen Weg, in dem die gesammelten Rohdaten prozessiert werden, unterschieden. Die untere Darstellung entspricht in ihrer Form dem Inhalt eines in SysML modellierten Aktivitätsdiagramms.

Mit dieser halbformalen Darstellung des Informationsflusses und der Überführung der PEGASUS-Methode [36] in einen Prozess nach dem gleichen Schema, konnte der Grundstein für die spätere Anwendung der SysML-Modellierung für die Darstellung der VVM-Gesamtmethode gelegt werden. Diese Arbeiten schafften dabei auch die Grundlage für weiterführende Diskussionen und Ausarbeitungen zur Darstellung der Gesamtmethode sowohl in SysML wie auch im Traceability Demonstrator.

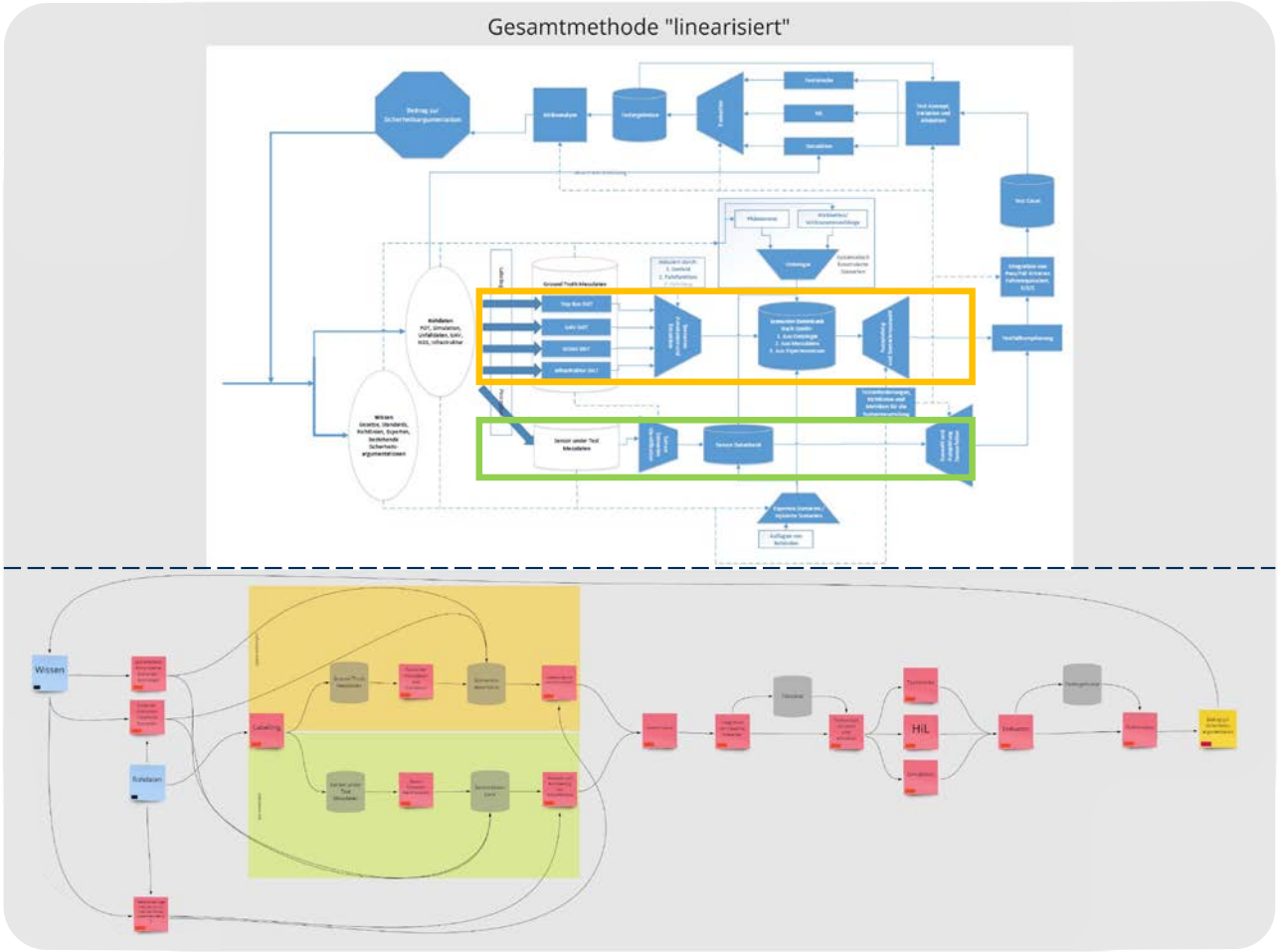


Abbildung 268: Darstellung des Informationsflusses (oben) und als „halbformale“ Prozessdarstellung (unten) in Anlehnung an SysML.

3.1.2.9.4.4 Baselining im Engineering Prozess

Das für das Baselining im Engineering Prozess kann das oben beschriebene Vorgehen ebenfalls mit einer kleinen Erweiterung genutzt werden. Die Erweiterung gliedert sich dabei in mehrere Stufen. Im ersten Schritt werden Projektergebnisse in einer erweiterten TP-Leiterrunde einem Review unterzogen. Ziel des Reviews ist die Projektergebnisse kritisch zu reflektieren und nach erfolgreichem Durchlaufen des Reviews als VVMethoden-Projektergebnis dem Gesamtprojekt zur Verfügung zu stellen (vgl. Projektinternes Baselining). Dies schafft dabei im zweiten Schritt auch eine Grundlage für einerseits die initiale Modellerstellung, da sich hier aus dem Results-Stack bedient werden kann und andererseits für die Diskussionen und Workshops mit den jeweiligen Stakeholdern. Die weiterführende Modellerstellung kann als dritter Schritt angesehen werden.

Wie oben beschrieben ist das Ziel des Vorgehens zum Baselining in Engineering Prozess die durchgängige Beschreibung der VVM-Methodik, sodass diese auch industriell nutzbar ist. Für die industrielle Anwendbarkeit der Ergebnisse ist es dabei essenziell, dass die beschriebenen Erkenntnisse nicht nur durchgängig sind, sondern auch auf deren Repräsentation einfach zugegriffen werden kann. Vor diesem Hintergrund wurde zusammen mit dem Projektmanagement und den TP-Leitern entschieden, die Dokumentation unter anderen in einem SysML-Modell durchzuführen. Das für die Modellierung verwendete Tool, bietet neben seinem nativen Format auch die Ausleitung in HTML, die mit einem aktuellen Internet-Browser geöffnet werden kann und in der im gesamten Modell lesend navigiert werden kann. Dies bietet auch außerhalb des

Projektes eine niedrige Einstiegshürde, wodurch auch Disseminationsaktivitäten unterstützt werden können. Da der Cameo Systems Modeller zusätzlich auch bereits bei einigen Projektpartnern eingesetzt wird, wird zusätzlich zum HTML-Export auch das native Format zur Verfügung gestellt, um den Projektpartnern zu ermöglichen, nach Projektende selbstständig an den Inhalten weiterzuarbeiten und diese in gegebenenfalls bereits in den Häusern existierende SysML-Modelle zu integrieren. Damit soll auch die industrielle Instanziierung und Verbreitung der VVM-Methodenergebnisse unterstützt werden.

3.1.2.9.4.5 Umsetzung im SysML-Modell

Für die konkrete, modell- bzw. SysML-basierte Umsetzung des „Baselining im Engineering Process“ wurde sich in Abstimmung mit dem Projektmanagement zu Anfang der Arbeiten an den Synchronisationspunkten der VVM-Methodik orientiert. Ziel ist dabei, deren Schnittstellen und Übergabeartefakte zu identifizieren, zu harmonisieren und somit die Durchgängigkeit über die Synchronisationspunkte (im weiteren Verlauf des Projektes und final im Projekt „Development & Operation – Global“ genannt) sicherzustellen.

Dazu wurden einerseits die Synchronisationspunktverantwortlichen identifiziert und andererseits zusammen mit einem Projektpartner eine Dokumentstruktur aufgesetzt und von PROSTEP überarbeitet, die es ermöglicht für jeden Synchronisationspunkt dessen Aktivitäten und die daraus resultierenden In- und Outputs textuell zu beschreiben. Abbildung 269 zeigt die für dieses Vorgehen verwendete generelle Struktur des Dokuments zu den Synchronisationspunkten. Die auf diese Art erzeugten Dokumente unterstützen ein einheitliches Verständnis über die Granularität der zu beschreibenden Artefakte. Zusätzlich zu den bereits gewonnenen und zur Verfügung gestellten Ergebnissen aus anderen Deliverables und aus dem Results-Board wurden, basierend auf diesen Inhalten, intensive Gespräche mit den Verantwortlichen für die Synchronisationspunkte sowie auch synchronisationspunktübergreifend geführt. Ziel war es einerseits den inneren Aufbau der Synchronisationspunkte weiter auszudetaillieren und anderseits die Schnittstellen zwischen den Synchronisationspunkten zu harmonisieren.

Dieses Vorgehen wurde in angepasster Version im weiteren Verlauf auch auf die weiteren Methodenbausteine, Development & Operation - Scenarios, Argumentation und Risk Management angewendet.

3 Synchronization Points of the VVM Method

3.1 Operational Concept

Main Author: NN

- **Goals** – a general description of what the constituent shall achieve
- **Inputs and Outputs**: Both a definition of the information going in and out, and the format in which this information is represented.
- **Activities, Methods, and Tools**
  - In- and Outputs of Subactivities of the Synchronization Points
  - Methods and Tools (Description of Methods and Tools; adequacy, consistency, and completeness of results)
  - Exemplification based on for FUC 2.3.

3.2 Criticality Analysis

Main Author: NN

- **Goals** – a general description of what the constituent shall achieve
- **Inputs and Outputs**: Both a definition of the information going in and out, and the format in which this information is represented.
- **Activities, Methods, and Tools**
  - In- and Outputs of Subactivities of the Synchronization Points
  - Methods and Tools (Description of Methods and Tools; adequacy, consistency, and completeness of results)
  - Exemplification based on for FUC 2.3.

Abbildung 269: Generelle Struktur des Dokuments zu den Synchronisationspunkten (im weiteren Verlauf des Projektes und final im Projekt „Development & Operation – Global“ genannt).

Die VVM-Gesamtmethode besteht neben den Synchronisationspunkten, (im Folgenden nur noch als „Development & Operation – Global“ bezeichnet) aus weiteren Bestandteilen. Abbildung 270 zeigt das finale dazu vorgestellte Schaubild, als Landing-Page im SysML-Modell. Im Reiter „Development & Operation – Global“ (oben links) sind die vormaligen Synchronisationspunkte als hellrosa Kästen dargestellt. Daneben enthält die Darstellung die weiteren Methodenbausteine, Development & Operation - Scenarios, Argumentation und Risk Management in schematischer Darstellung.

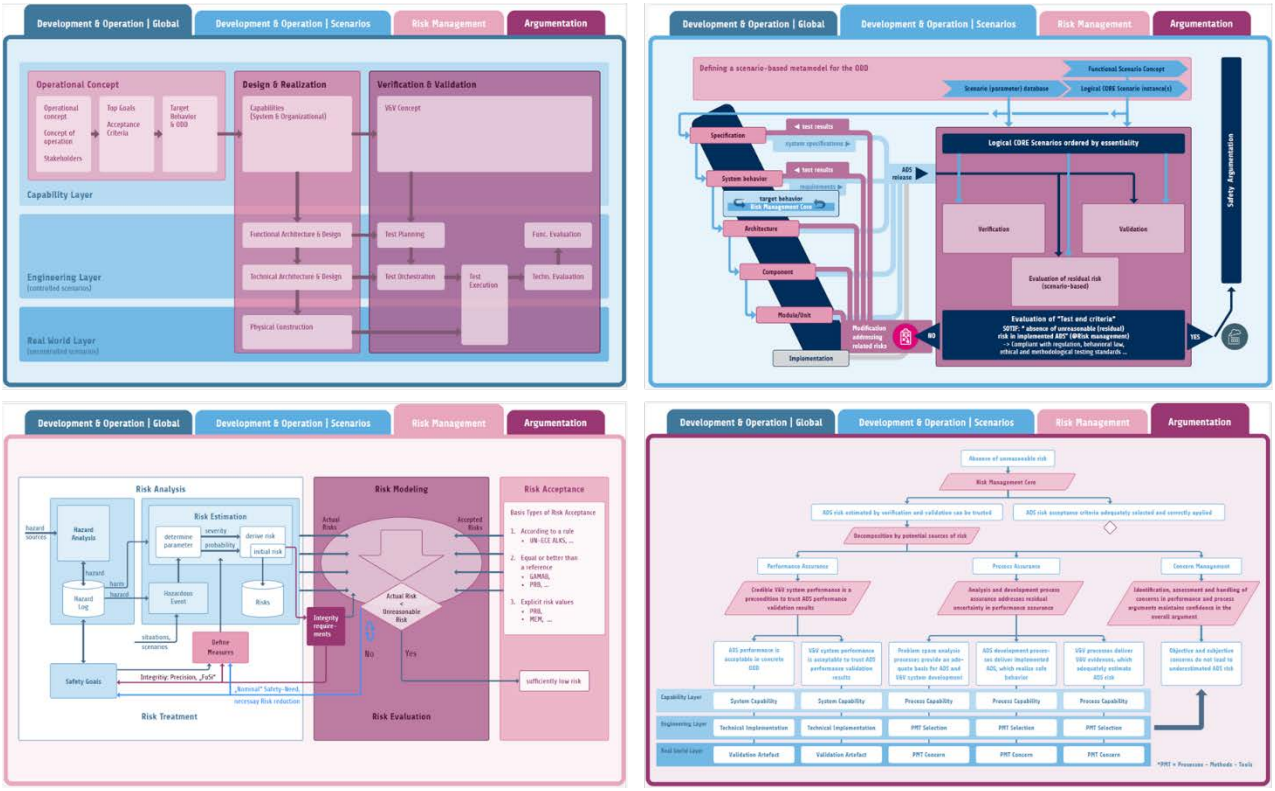


Abbildung 270: VVM-Gesamtmethode – Methodenzusammenführung (Landing-Page – SysML-Modell).

Die in Abbildung 270 dargestellten Elemente, die zur Gesamtstruktur der Methode beitragen wurden ebenfalls in dieser Form in das SysML-Modell als Landing-Page für die HTML-Ausleitung übernommen. Die Darstellung der Hauptelemente als Einstiegspunkt in Form einer Landingpage wurde vor allem in dieser Form für eine spätere Veröffentlichung des Modells gewählt. Sie ermöglicht einen mit dem Management und dem Projekt abgestimmten niedrigschwelligen Einstieg über das Modell in die Methode, da dieselben Elemente auch auf den zugehörigen Referenzseiten, Postern und in den Vorträgen des Abschlussevents verwendet wurden und damit ein eindeutiger Wiedererkennungswert garantiert ist.

Für die Integration der tieferen, detaillierteren Ebenen der Gesamtmethode hat PROSTEP die Hauptelemente der VVM-Gesamtmethode nicht nur graphisch, wie in Abbildung 270 dargestellt, in das Modell aufgenommen. Sie wurden ebenfalls als Top-Level-Ebene in das SysML-Modell integriert. Die formale Darstellung der Hauptelemente der VVM-Gesamtmethode mit ihren Zusammenhängen untereinander ist in Abbildung 271 abgebildet. Diese Darstellung dient zum einen dazu, den Einstieg in die Diskussionen und Abstimmungen zu erleichtern, da direkt am Modell über die globalen Schnittstellen zwischen den Hauptelementen der Methode diskutiert werden kann. Damit werden alle neu gewonnenen Erkenntnisse direkt und zentral an einem Ort und auch für die Vertreter der anderen Hauptelemente sichtbar dokumentiert. Zum anderen erleichtert die formale Schreibeweise die Sicherstellung der Durchgängigkeit der Schnittstellen, da die Übergabe- und Austauschobjekte, sowie die Richtung, in die sie übergeben werden, in dieser Darstellung direkt sichtbar werden.

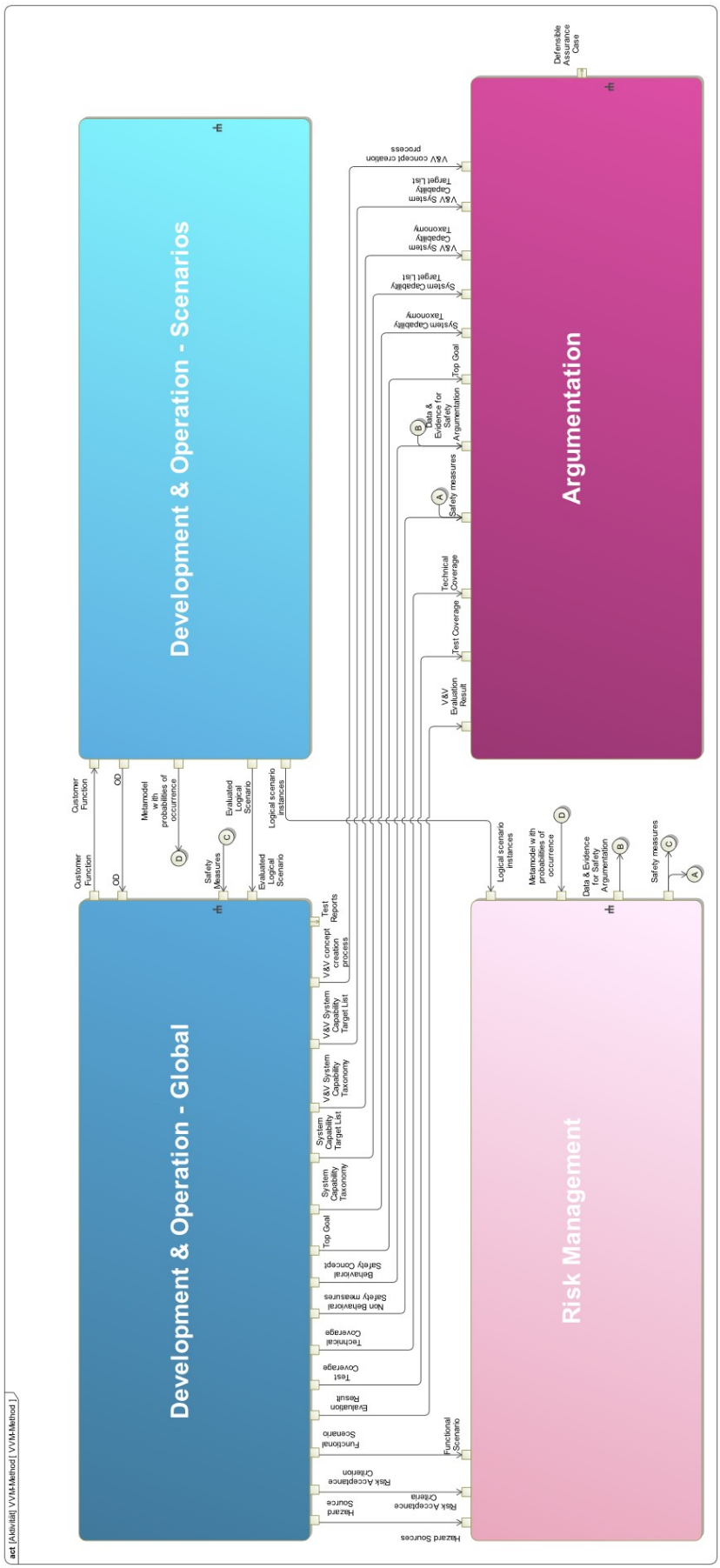


Abbildung 271: Modellierung der Hauptelemente der VVM-Gesamtmethode mit deren Zusammenhängen.

Basierend auf den verfügbaren Dokumenten, Projektinhalten und in Abstimmung mit den Verantwortlichen für jeweiligen Methodenbausteine wurde ein übergreifendes SysML-Modell der Gesamtmethode durch PROSTEP erstellt. Dabei sind für die jeweiligen Hauptelemente der VVM-Methode detailliertere Beschreibungen im Modell erstellt worden. Diese sind jeweils auch wieder durch Aktivitäten mit deren Inputs und Outputs beschrieben. Somit kann auch das Zusammenspiel innerhalb der Hauptelemente der VVM-Methode durchgängig beschrieben und dokumentiert werden.

Dieses Vorgehen bietet die Möglichkeit, direkt die Schnittstellen und Übergabeartefakte konsistent zu dokumentieren und etwaige Unstimmigkeiten zu identifizieren. Anhand des auf diese Weise erstellten immer weiterwachsenden Modells, wurden zyklisch Diskussionen hinsichtlich Durchgängigkeit der gesamten Methode mit den Verantwortlichen geführt. Durch die Kapselung innerhalb der Methodenbausteine in Form von einzelnen miteinander verbundene Aktivitäten war es zudem möglich, einzelne Teilbereiche auch in unterschiedlichem Detaillierungslevel zu beschreiben, da die globalen Schnittstellen zwischen den Aktivitäten immer auf der höherliegenden Ebene eindeutig beschrieben wurden und somit der Detaillierungsgrad im Inneren diese nicht beeinflusst.

Dieses Vorgehen wurde speziell, aber nicht ausschließlich im Hauptelement „Development & Operations – Global“ auf mehreren Ebenen angewendet. Dies garantiert zusätzlich eine einfache Verständlichkeit und Übersichtlichkeit der modellierten Inhalte, da nur ein überschaubarer Anteil an Informationen in einem Diagramm beschrieben wird und detaillierte Informationen eine Ebene tiefer zu finden sind. Dieses Top-Down Vorgehen ermöglicht es zudem, wenn gewünscht nur einzelne Methodenbestandteile detailliert zu betrachten und trotzdem den Gesamtzusammenhang innerhalb der Methode zu erfassen. Die abstrakteren Beschreibungen sind aufgrund der durchgängigen Schnittstellen auch mit deutlich detaillierten Aktivitäten eindeutig und konsistent verbunden.

Abbildung 272 zeigt exemplarisch für dieses Vorgehen den Zusammenhang verschiedener Modell-/Methodenebenen. Ganz oben wurde das Hauptelement „Development & Operations – Global“ ausgewählt. Eine Ebene tiefer findet man sich auf den dieses Hauptelement strukturierenden „Layern“, Capability, Engineering und Real World Layer (in Blautönen) wieder. Auch hier wurden zur Übersichtlichkeit und für das Verständnis die Zusammenhänge innerhalb des Hauptelements der Methode noch relativ abstrakt beschrieben. Man erkennt aber auch hier, dass die Inputs und Outputs der höheren Ebene vollständig in dieser Darstellung auftauchen und von Methodenelementen verwendet werden. Eine weitere Ebene tiefer sind die konkreten Kernaktivitäten innerhalb des Hauptelements beschrieben. Diese wurden im Rahmen des Projektes auch als Synchronisationspunkte beschrieben und haben zum Teil direkten Bezug zu einzelnen Teilprojekten. Auch hier sind zur besseren Einordnung wieder die „Layer“ vollständig mit aufgeführt. Auf der letzten hier dargestellten Ebene wird der Aufbau der „Criticality Analysis“ beschrieben. Man erkennt auf dem linken Rand des Diagramms die Übergabeobjekte, die an den Schnittstellen der „Criticality Analysis“ von anderen Methodenbausteinen für deren interne Nutzung in der „Criticality Analysis“ geliefert werden. Die Objekte, die nach der Prozessierung bereitgestellt werden, sind am rechten Rand des Diagramms dargestellt und werden über diese Schnittstelle für andere Methodenbaustein zur Verfügung gestellt. Im Diagramm selbst ist der Ablauf innerhalb der „Criticality Analysis“ dargestellt. Dem Diagramm ist somit zu entnehmen, wie die einzelnen Aktivitäten aufeinander folgen und Objekte durch die Aktivitäten laufen und prozessiert werden.

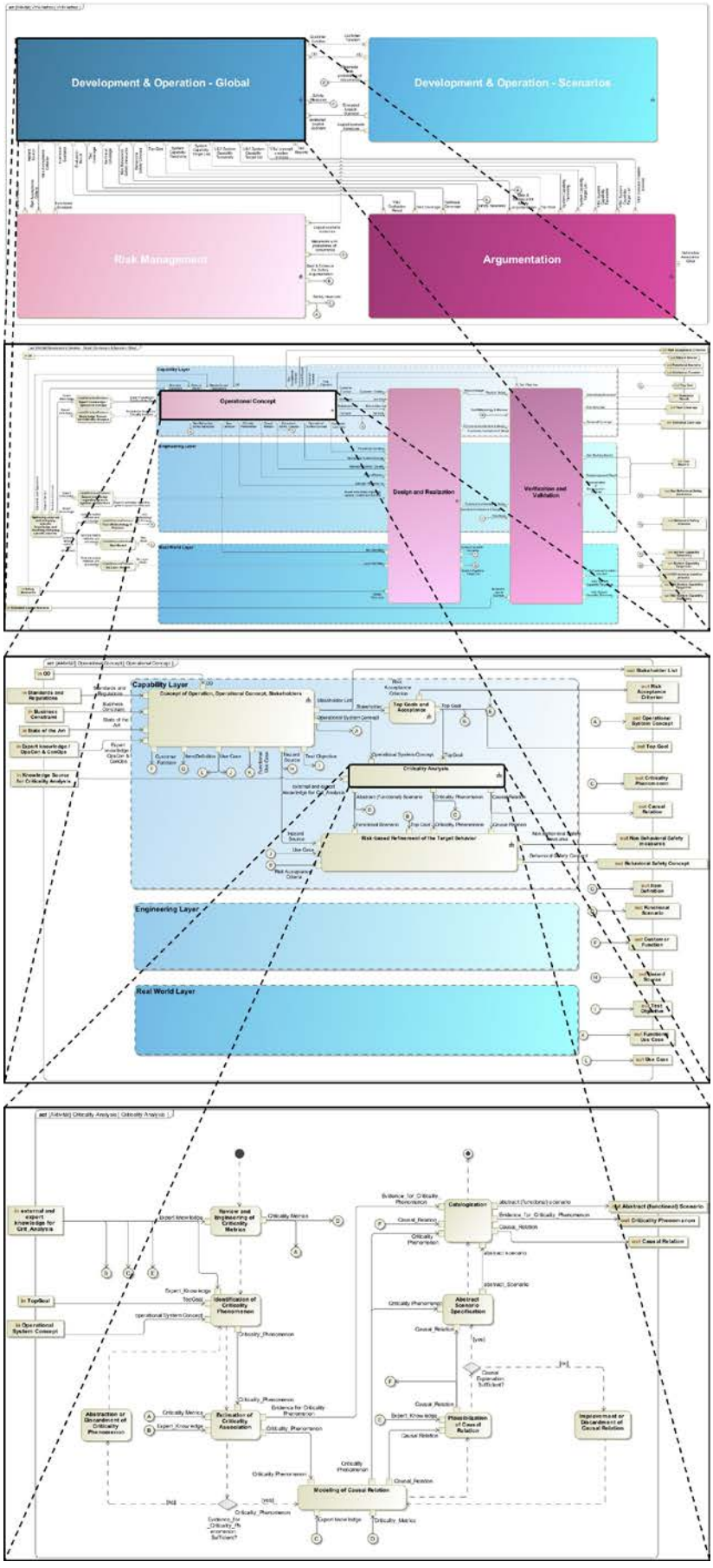


Abbildung 272: Darstellung des Zusammenhangs verschiedener Modell-/Methodenebenen.

Der in Abbildung 272 dargestellte Aufbau des Modells zeigt primär die einzelnen Aktivitäten und Prozesse sowie deren Ablauf, die Zusammenhänge und die Austausch- beziehungsweise Übergabeobjekte zwischen den Prozessschritten.

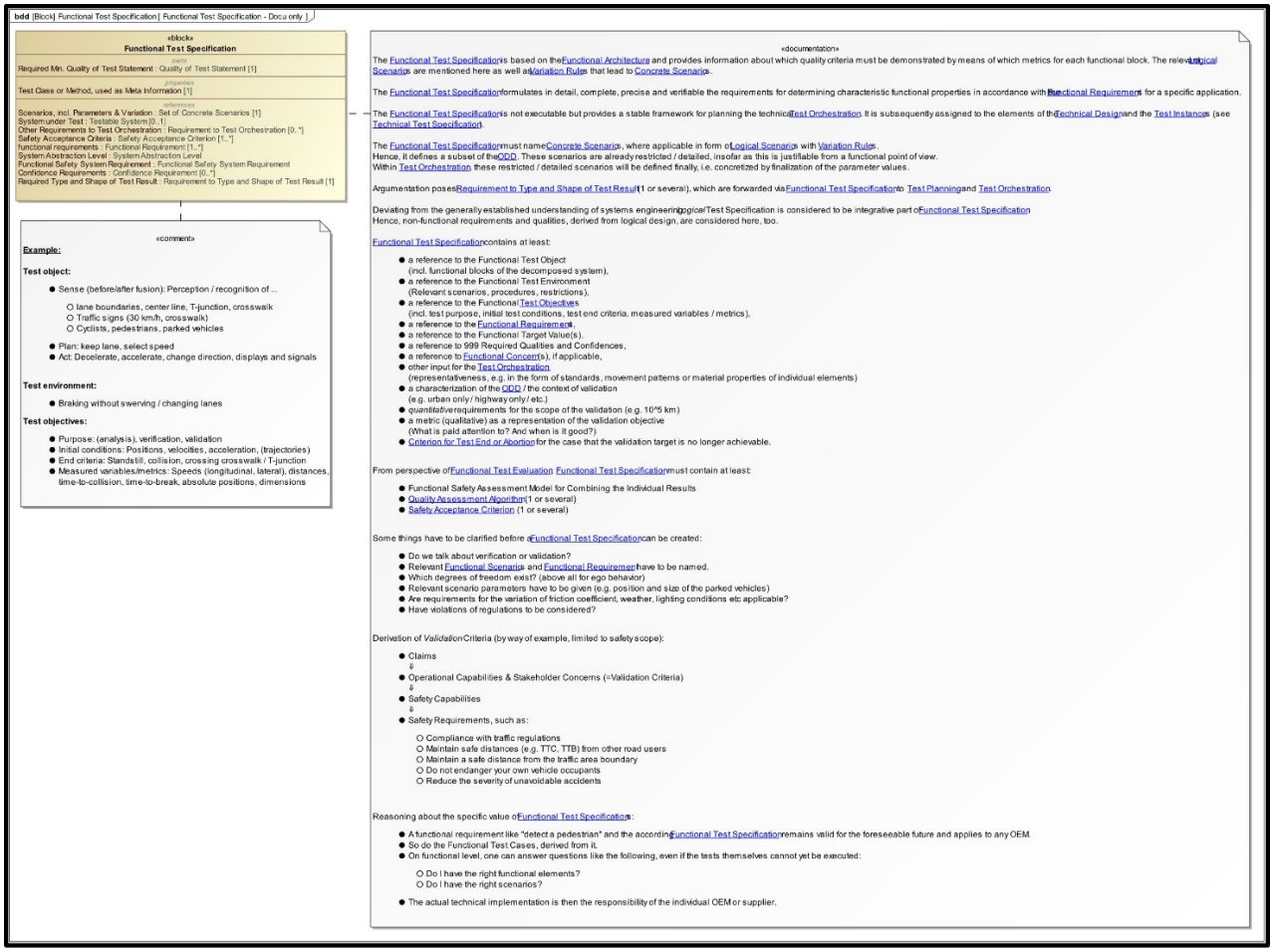
Im Rahmen der Modellierung und der Erstellung des Modells hat sich gezeigt, dass dies eine sehr gute Übersicht über die einzelnen Bestandteile der VVM-Methode liefert, jedoch bestimmte Abhängigkeiten und Zusammenhänge auf diese Weise nicht vollständig erfasst werden. Aus diesem Grund wurden neben den reinen Aktivitätsdiagrammen weitere Diagrammarten mit in das Modell aufgenommen, mit deren Hilfe es möglich ist, die weiteren Zusammenhänge abzubilden.

Als einfache Erweiterung zum ursprünglichen Vorgehen sind Diagramme enthalten, die Anforderungen an bestimmte Prozesselemente oder Übergabeobjekte enthalten bzw. selbst Übergabeobjekte sind. Darüber hinaus wurden Diagramme eingeführt, welche die direkten Beziehungen und den Aufbau von bestimmten Übergabeobjekten direkt beschreiben können. Dies wurde vor allem bei Objekten durchgeführt, die selbst aus verschiedenen Einzelobjekten bestehen, um diese als Oberobjekt von einer Aktivität zur nächsten übergeben zu können, ohne alle Einzelteile übergeben zu müssen. Des Weiteren kam dieses Vorgehen zum Einsatz, wenn Objekte komplexere Zusammenhänge zu anderen Objekten besitzen. In beiden Fällen wird dadurch die Übersichtlichkeit und Verständlichkeit der Modelle erhöht. Abbildung 273 (unten) stellt exemplarisch ein solches Diagramm dar.

In diesem Diagramm wird zentral das Objekt „Technical Test Specification“ beschrieben. Man erkennt, dass die „Technical Test Specification“ aus mehreren Objekten besteht. Dazu gehören „Test Case“, „Initial Assessment of Success of Test Sequence”, “Test Infrastructure” und „Test Sequence Specification”, sowie weitere als “References” und Objekte. Man kann hieraus somit direkt ablesen, welche Inhalte in der „Technical Test Specification“ beschrieben werden. Weiterhin ist beispielsweise, wenn man den Abhängigkeiten nach oben folgt, zu entnehmen, dass die „Test Sequence Specification“ aus einem „Test Procedure“ besteht, welches wiederrum ein „Criterion for Test End or Abortion“ enthält, was sich aus der „Required Quality and Confidence“ und dem zugehörigen Requirement „Confidence Requirement“ ableitet.

Mit zunehmender Modellkomplexität erschien er sinnvoll solche Zusammenhänge nicht nur zu modellieren, sondern in ausgewählten Fällen auch textuell im Modell zu dokumentieren, um gerade bei zentralen Objekten die Einstiegshürde gering zu halten, beziehungsweise ein Nachschlagewerk zusätzlich zur Modellierung zu haben. Ein solches Beispiel ist in Abbildung 273 (oben) dargestellt. In der textuellen Beschreibung der „Functional Test Specification“, sind zudem Links (in Blau) zu einzelnen anderen Objekten hinterlegt, um auch hier eine einfache Navigation im Modell zu ermöglichen.

Mit Fortschreiten des Modellaufbaus wurden einzelne Teile des Modells von einigen Arbeitsgruppen darüber hinaus auch als konkretes Arbeitsmedium zur Dokumentation und Diskussion etabliert. Durch die Kapselung innerhalb der Methodenbausteine konnte die Ergebnisse direkt genutzt und die erarbeiteten Modelle direkt in die zugehörigen Elemente integriert werden, ohne das allgemeine Vorgehen anpassen oder überarbeiten zu müssen, selbst wenn der Detaillierungsgrad hierbei teilweise deutlich höher war, als dies ggf. in anderen Bausteinen der Fall war. Die Konsistenz des Modells war weiterhin durch die globalen Schnittstellen sichergestellt.



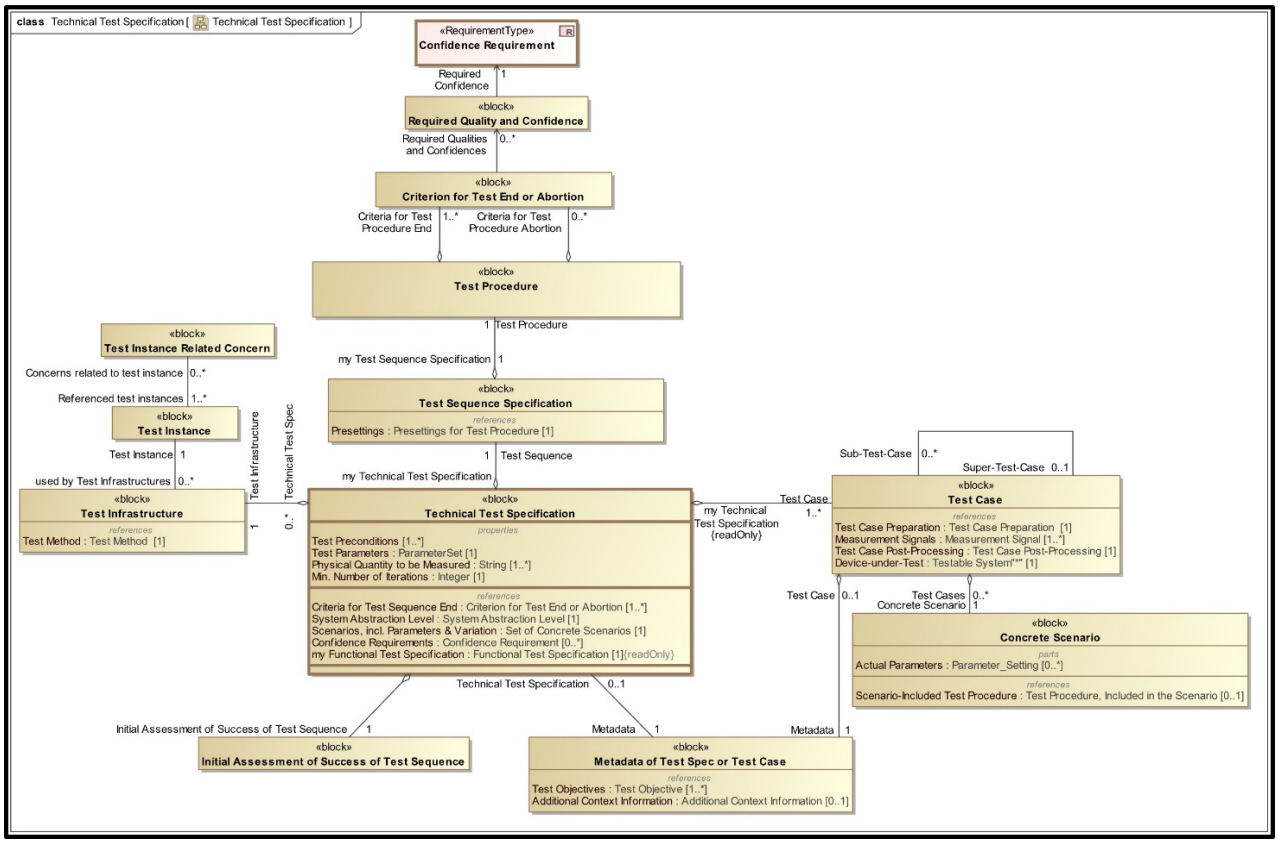


Abbildung 273: Beispiel für weiterführende Zusammenhänge und Dokumentation im Modell.

3.1.2.9.4.6 Ausleitung zur Dissemination und weiteren Verwendung nach Projektende

Für die spätere Dissemination, als Vorbereitung für die Nutzung auf dem Abschlussevent von VVMethoden und die weitere mögliche Verwendung bei Projektpartnern wurde zusammen mit dem Projektmanagement und den TP-Leitern, wie oben beschrieben, beschlossen, dass das Modell als HTML-Export zu Verfügung gestellt wird.

Zusätzlich bietet diese Form der Veröffentlichung auch einen gewissen Schutzmechanismus. Da der Nutzer nur lesende Rechte hat, können keine Veränderung am Modell vorgenommen werden, wenn dieses VVMethoden-fremden Personen, zum Beispiel auf dem Abschlussevent oder im Austausch mit externen Partnern auf der VVMethoden Homepage (https://cameo.vvm-projekt.de/), zur Verfügung gestellt wird. Projektintern wird auch das proprietäre Format mit allen Änderungsmöglichkeiten zur Verfügung gestellt.

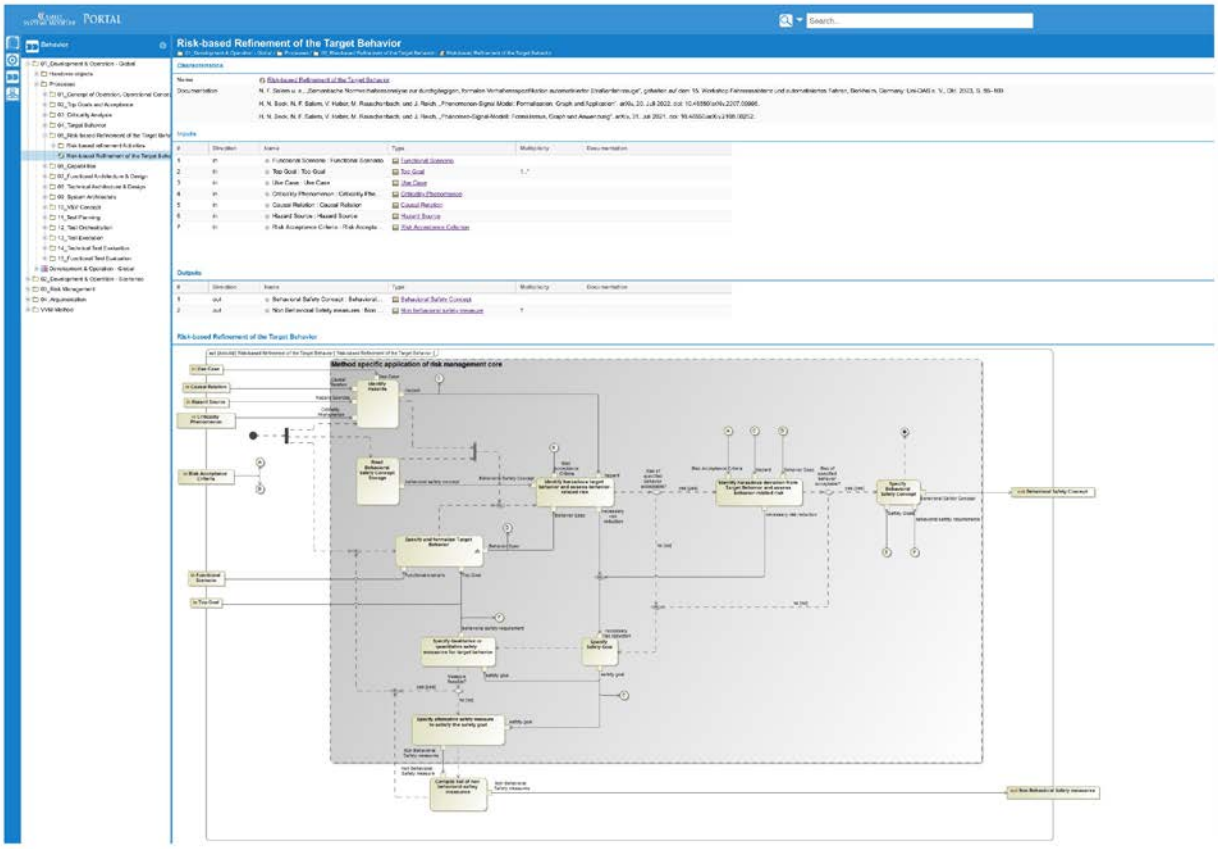


Abbildung 274: HTML-Ausleitung des SysML-Modells, Ansicht im Browser („Risk-based Refinement of the Target Behavior“).

Abbildung 274 zeigt die Ausleitung in der HTML-Ansicht. Man erkennt im unteren Teil das graphische Modell des „Risk-based Refinement of the Target Behavior“. Am linken Rand befindet sich der Navigationsbereich, in dem durch die gesamte VVM-Methode navigiert werden kann. Im mittleren Bereich der Abbildung sind die In- und Outputs des Diagramms hinterlegt. Im oberen Teil können weiterführende Inhalte dargestellt werden, wie z.B. in diesem Fall weiterführende Informationen in Form von Links auf Veröffentlichungen. Die einzelnen Elemente des Diagramms sowie die In- und Outputs sind dabei „klickbar“, sodass damit durch die Gesamtmethode navigiert werden kann.

Darüber hinaus wurde im Projekt diskutiert, in welcher Form die Inhalte schriftlich zum Beispiel für Deliverables oder Berichte nachhaltig dokumentiert werden können. Abbildung 275 zeigt eine mögliche von PROSTEP vorgeschlagene Ausleitung einer solchen Dokumentation direkt aus dem SysML-Modell, die als PDF unveränderbar abgelegt werden kann.

Auch in dieser Dokumentation ist das im Modell erstellte Diagramm enthalten (vgl. Abbildung 275 links). Darüber hinaus sind auch hier wieder die einzelnen Aktivitäten der Methodenelemente dokumentiert und tabellarisch deren In- und Outputs aufgeführt. Zusätzlich sind in der Dokumentation die erläuternden Inhalte sowie die weiterführenden Verweise, soweit im Modell enthalten, verfügbar. Die Ausleitung enthält somit alle wesentlichen Inhalte des Modells in verschriftlichter Form und kann als Art „Beipackzettel“ zum Modell angesehen werden.

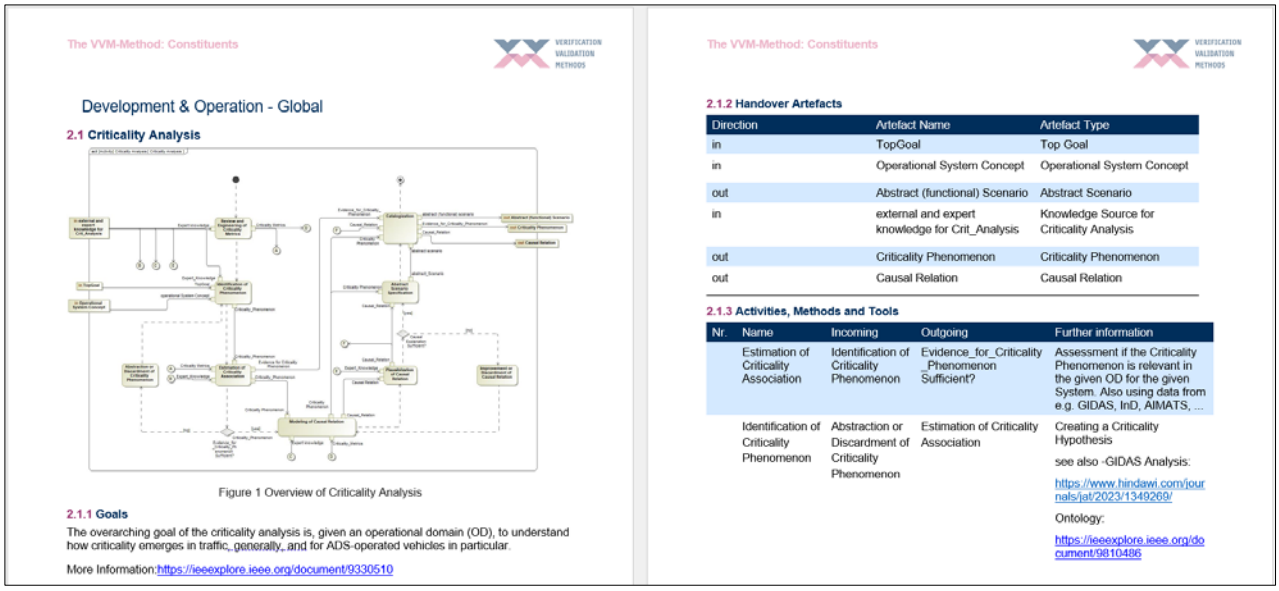


Abbildung 275: Darstellung der Inhalte aus dem SysML-Modell in verschriftlichter Form z.B. als Worddokument oder PDF (hier dargestellt: Criticality Analysis).

3.1.2.9.5 Abbildung der Gesamtmethode im Traceability Demonstrator

Zusätzlich zur von PROSTEP durchgeführten Dokumentation der Gesamtmethode im SysML-Modell, wurde die Abbildung der Methode im, in dem Projekt entwickelten Traceability Demonstrator TRACY vorgenommen. Das Ergebnis wurde ähnlich, wie bereits auf dem VVM-Halbzeitevent, auch als Showcase für das Abschlussevent verwendet.

Dabei soll durch die Nutzung von TRACY die VVM-Gesamtmethode noch einmal in einer alternativen Darstellung einem breiten Publikum auf dem Abschlussevent zugänglich gemacht werden. Durch seine graphische Benutzeroberfläche bietet es einen leichten Einstieg in die Inhalte, der weniger formal gestaltet ist als dies im SysML-Modell für die Gesamtmethode der Fall ist.

Darüber hinaus wurden beide Darstellungen der VVM-Gesamtmethode dahingehend entwickelt, dass die Ergebnisse des Vorgehens dem Projekt und insbesondere den VVM-Industriepartnern nach Projektende zur Verfügung gestellt werden können. Für die industrielle Anwendbarkeit der Ergebnisse ist es dabei essenziell, dass die beschriebenen Erkenntnisse nicht nur durchgängig sind, sondern auch auf deren Repräsentation einfach zugegriffen werden kann. Vor diesem Hintergrund bietet die Umsetzung im Traceability Demonstrator die Möglichkeit eines Exports in

XML, sowie auch eine zeitlich beschränkte Nutzung des Demonstrators nach Projektende durch die Partner.

Zusätzlich bietet der Traceability Demonstrator für eine spätere konkrete Anwendung in den Firmen, neben der reinen Darstellung des Prozesses der VVM-Gesamtmethode und dessen Entwicklungsartefakte auch die Möglichkeit unterschiedliche Revisionsstände abzubilden, um den Fortschritt der Entwicklung nachvollziehbar zu gestalten. Dies entspricht dem Gedanken des Konfigurationsmanagements nach ISO 10007 [116]. Hierbei ist es auch möglich, speziell konkrete Dokumente und Entwicklungsartefakte in TRACY aus verschiedenen Fremdsystemen zu verlinken, um die konkrete Entwicklung entlang der Methode zu unterstützen und die dabei vorhandenen Abhängigkeiten auch graphisch nachvollziehbar zu veranschaulichen.

Im Folgenden soll kurz auf das Thema Konfigurationsmanagement und Traceability eingegangen werden sowie die Kernfunktionalitäten der Traceability Demonstrators vorgestellt werden.

3.1.2.9.5.1 Traceability im Kontext des Konfigurationsmanagements

Traceability ist die kontextspezifische Verknüpfung von Artefakten (Dokumente, Strukturen, Unterstrukturen usw. und zugehörige Metadaten) über Trace-Links. Alle Trace-Links und die zugehörigen Artefakte bilden Kanten und Knoten eines Graphen, der z.B. für effiziente Analysen genutzt werden kann.

Die Traceability ist besonders relevant bei der Entwicklung sicherheitskritischer Systeme und bei vorgeschriebenen Audits, z. B. nach ISO 26262, Automotive SPICE und EN 50128. Eine gemeinsame Anforderung dieser Richtlinien ist, dass kritische Anforderungen verifiziert werden müssen und das diese Verifizierung durch Rückverfolgbarkeit transparent gemacht werden muss. Heute sind die entsprechenden Prozesse dokumentengetrieben - was zeitaufwändig, fehleranfällig usw. ist.

Die Vorteile der Realisierung von Traceability sind z.B. (system-, orts-, organisations-) unabhängige Verknüpfungen von Artefakten, persistente Beziehungen, Änderungseinflussanalysen, Abdeckungsanalysen, Projektstatusanalysen, Wiederverwendung von Produktkomponenten, Testoptimierung. Aufgaben mit Traceability-Unterstützung sind 24% schneller und 50% korrekter [117].

Im Kontext des hochautomatisierten Fahrens stehen sowohl sicherheitskritische wie komplexe Systeme im Fokus, an die hohe Ansprüche an Qualität und Zuverlässigkeit gestellt werden. Daher nimmt auch hier das Thema Traceability eine wichtige Rolle ein. Der Grundgedanke der Traceability bezieht sich auf das Konfigurationsmanagement. Abbildung 276 stellt die einzelnen Bereiche des Konfigurationsmanagement gemäß der ISO 10007 [116] dar.

ISO 10007 „Quality management – Guidelines for configuration management“ [116] definiert:

> *Configuration management is a **management activity** that applies technical and administrative direction over the life cycle of a product and service, its configuration **identification** and **status**, and related product and service configuration **information**.*
>
> *Configuration management documents the product or service configuration. It provides identification and **traceability**, the **status of achievement** of its physical and functional requirements, and **access** to accurate **information** in **all phases of the life cycle**.*

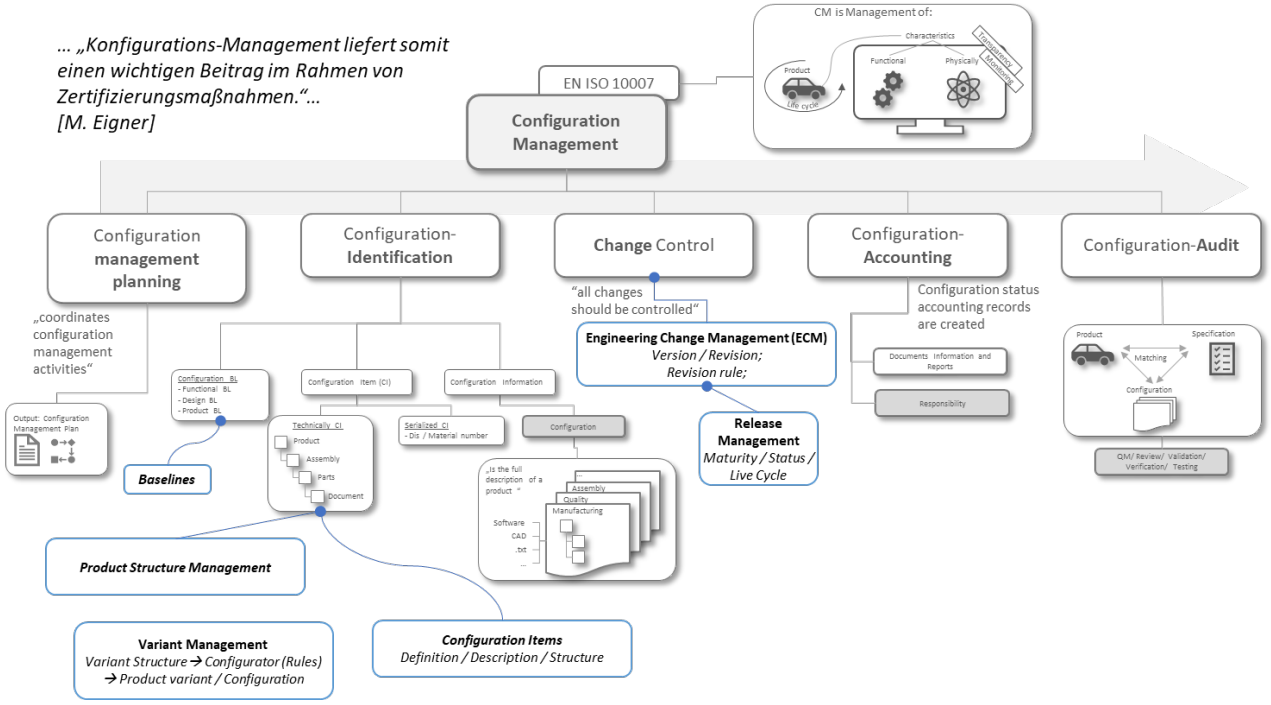


Abbildung 276: Konfigurationsmanagementbereiche gemäß ISO 10007 [116].

Zum Nachweis der oben angesprochenen Sicherheit und Qualität eines hoch automatisierten Fahrzeugs ist es unabdingbar, seine exakte Konfiguration zu dokumentieren, die Zusammenstellung und Konfiguration der zugehörigen Entwicklungsartefakte zu managen und jederzeit den Nachweis führen zu können, wie jedes einzelne Artefakt zu Stande gekommen ist. Diese Traceability ist auch eine elementare Grundlage für die Glaubwürdigkeit der Entwicklungsergebnisse.

3.1.2.9.5.2 Traceability Demonstrator „TRACY“

Ohne die Unterstützung einer leistungsfähigen Software ist es nahezu unmöglich, die Vielzahl an Prozessen und Artefakten sowie ihrer wechselseitigen Abhängigkeiten unter Kontrolle zu halten. Daher wurde im Rahmen von VVMethoden eine solche Software als Demonstrator für Traceability von PROSTEP entwickelt. TRACY ist ein neutraler Software-Demonstrator einer Traceability-Software, die in den öffentlich geförderten Projekten SET Level und VVMethoden entwickelt wurde und für diese bereitgestellt wurde.

Für die erforderliche Dokumentation der VVM-Methode wurde TRACY als ein innovatives, auf die spezifische Komplexität zugeschnittenes Tool eingesetzt. Es kann über Baselines Traceability ermöglichen, so dass zu jeder Zeit sicher nachgewiesen werden kann, welche Annahmen, Modelle, Daten und Parameter unter Zuhilfenahme welcher Software eingesetzt wurden. Dazu verknüpft das Tool die entsprechenden Daten und ermöglicht auch das geordnete Ablegen von Informationen, für die es nach aktuellem Stand der Technik noch kein System gibt. Es bildet somit eine technologische Grundlage für die Schaffung einer Baseline über alle relevanten Artefakte. Damit setzt TRACY die Grundprinzipien des Konfigurationsmanagements nach ISO 10007 [116] (insbesondere Trace-Links) um.

Das Traceability-Tool dient der fachgebietsübergreifenden Zusammenarbeit und kann Informationen aus unterschiedlichsten Datenquellen zusammenstellen ohne Eingriff in diese Datenquellen zu nehmen. Die Autorensysteme können damit leicht an notwendige Veränderungen

und Innovationen angepasst werden und es kann flexibel auf Änderungen reagiert werden. Abbildung 277 zeigt die finale Ausbaustufe des Traceability Demonstrators TRACY in VVMethoden.

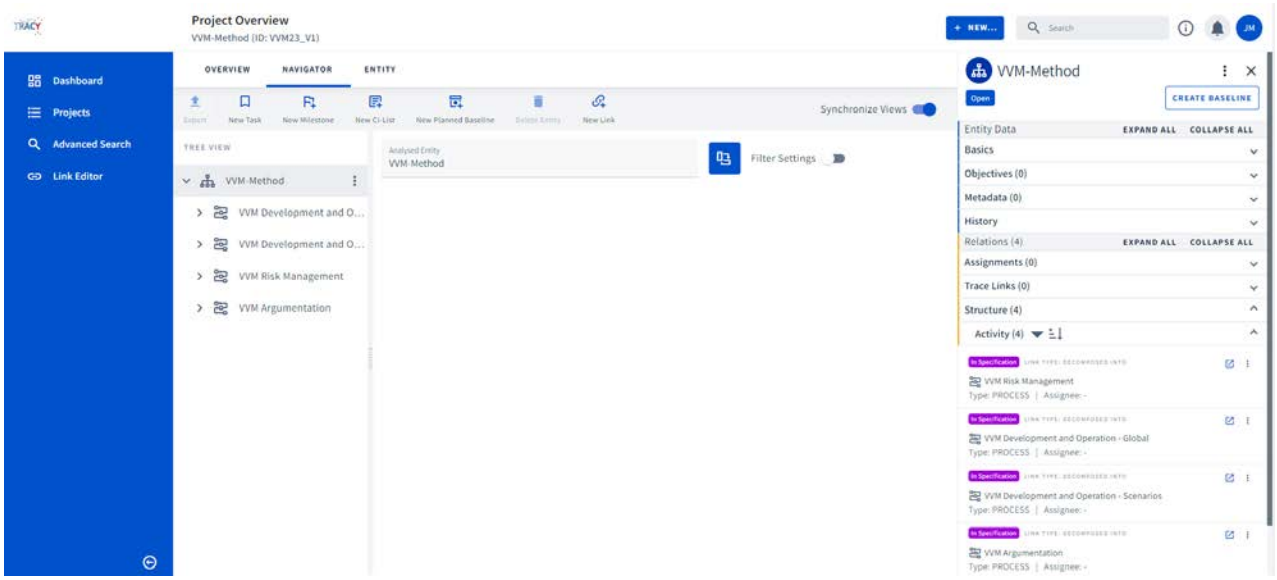


Abbildung 277: Finale Ausbaustufe des Traceability Demonstrators in VVMethoden.

TRACY – Use Cases und Funktionalitäten

Ein Traceability-Tool muss die zentralen Zusammenhänge abbilden und damit die Rückverfolgbarkeit zwischen Argumentation und Entwicklungsprozessen deutlich machen. Zentrale im Projekt geforderte Use Cases für eine solche Software sind:

Compliance sicherstellen

- Informationen aufbereiten und speichern
- Prozesse unterstützen
- Revisionssicherheit, Auditierung

Komplexität beherrschen

- Auswirkungsanalyse
- Reifegrad dokumentieren
- Nachverfolgung & Steuerung
- Änderungen überwachen

Effizienz steigern

- Suche & Wiederverwendung
- Front-loading
- Automatisierung
- Zusammenarbeit

Qualität sichern

- Richtige Informationen, zur rechten Zeit etc.
- Konsistenz
- Vollständigkeit

Um die oben beschriebenen Use Cases zu adressieren und abzudecken, wurden in TRACY u.a. folgende Funktionalitäten realisiert:

- User-Management
- Rollen- und Rechte-Management
- User-spezifische Cockpits und Sichten
- Workflow zur Qualitätssicherung
- Realisierung von Notifications (Hinweise, z. B. wenn einem Benutzer ein neuer Task zugewiesen wurde)
- Anlegen und Suchen von Artefakten (inkl. Metadaten)
- Anlegen von Trace-Links zwischen Artefakten (Relationen)
- Realisierung einer Baselining-Funktionalität
- Möglichkeiten zur Durchführung dynamischer Impact-Analysen
- Grafische Benutzeroberfläche (GUI)
- Grafische Darstellung von verwalteten Artefakten und ihrer Relationen
- Darstellungs- und Filtermechanismen in der Graph-Ansicht
- Befüllen von TRACY mit Projektdaten
- Einbindung weiterer Systeme nach dem Standard OSLC (beispielsweise DOORS)
- Cloudfähigkeit des Traceability-Demonstrators

TRACY – Artefakt-Arten

Zur besseren Strukturierung der Dokumentation der Methode und der Übergabeartefakte wurden in TRACY verschiedenste Klassifizierungen der Artefakt-Arten implementiert. TRACY unterstützt u.a. folgende Klassifizierungen von Artefakten:

- Activity
- Requirement
- Design specification
- Test Case
- Scenario
- Model
- Parameter Set
- Simulation Result
- Verschiedenste importierbare SysML-Klassen
- uvm.

Jedes dieser Artefakte kann zusätzlich mit verschiedenen *Metadaten* angereichert werden. Darüber hinaus können unterschiedliche Abhängigkeiten, die sogenannten Trace-Links, zwischen den Artefakten gesetzt werden. Damit entstehen aus den Artefakten und den zugehörigen Beziehungen navigierbare Tripple-Graphen.

3.1.2.9.5.3 Umsetzung im Traceability-Demonstrator

Ebenso wie bei der oben beschriebenen Modellierung in SysML, wurde auch der Traceability Demonstrator teilweise als Arbeitsmedium zur Dokumentation von Projekt- oder Workshopergebnissen eingesetzt, um die Anwendbarkeit zur Unterstützung des „Baselinings im Engineering Process“ zu zeigen und zu evaluieren. Ziel war dabei unter anderem auch projektspezifische Anforderungen an den Traceability Demonstrator durch dessen konkrete Nutzung zu definieren. Dies geschah, um bereits frühzeitig eine Akzeptanz des Demonstrators für die Anwendung zur Dokumentation der Gesamtmethode und der Darstellung von Inhalten auf dem Halbzeitevent zu schaffen. Die Anforderungen ergaben sich dabei sowohl aus der Anwendung sowie aus konkreten Rücksprachen mit Projektpartnern. Abbildung 278 zeigt ein Bespiel der Umsetzung der Ergebnisse eines Projektmeetings im Traceability Demonstrator.

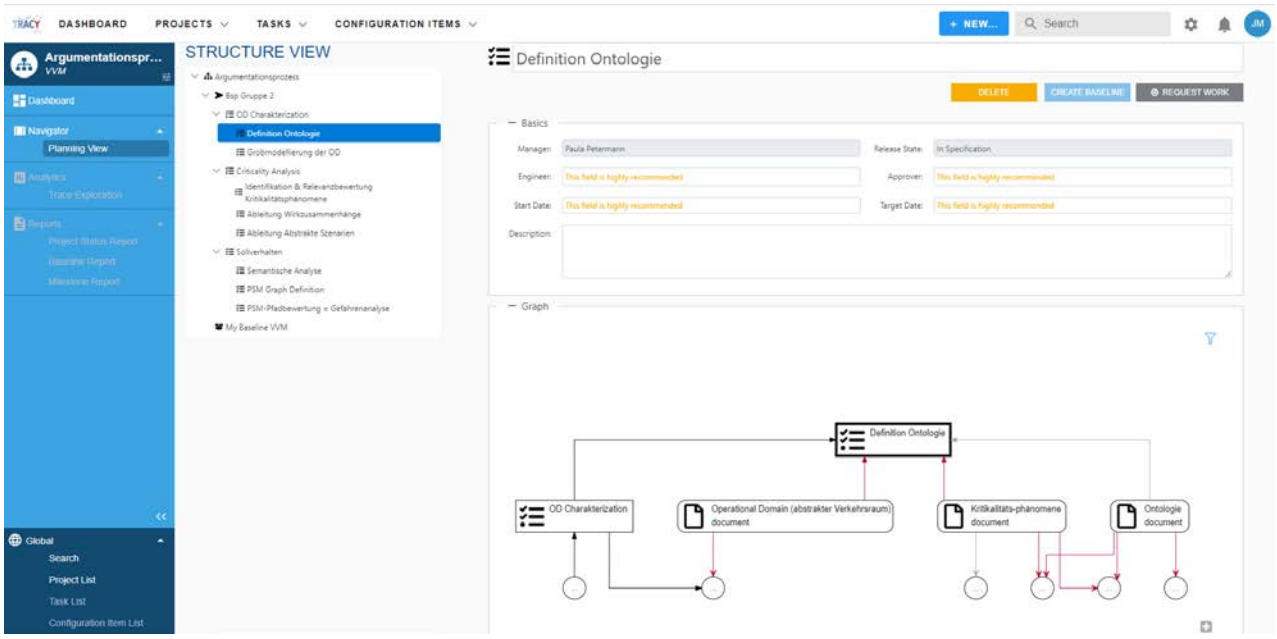


Abbildung 278: Beispielhafte Umsetzung der Ergebnisse eines Projektmeetings in TRACY.

Nach den initialen Arbeiten wurden als Startpunkt für die Umsetzung im Traceability Demonstrator die Prozesse und Artefakte innerhalb des Teilprojektes 3 gewählt. Die hier gewonnenen Erkenntnisse wurden im Folgenden dann auf die weiteren Elemente der Methode angewendet. Abbildung 279 zeigt exemplarisch einen Ausschnitt der durchgängigen Argumentationskette im Teilprojekt 3 und die Verbindung mit anderen Teilprojekten.

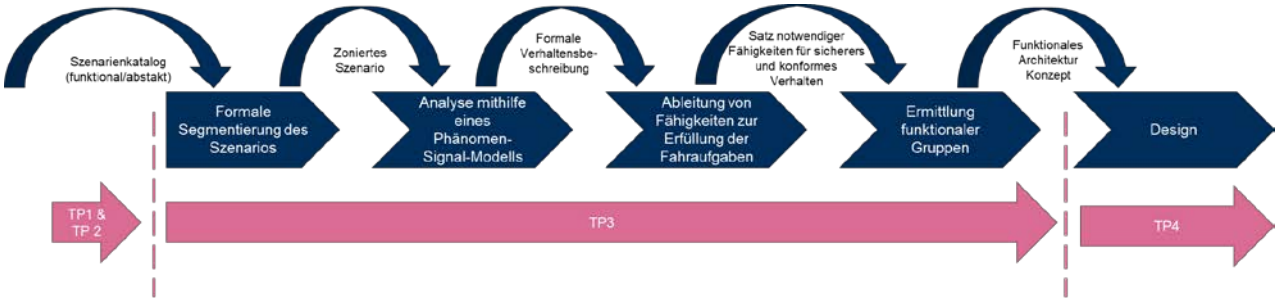


Abbildung 279: Ausschnitt der durchgängigen Argumentationskette im Teilprojekt 3 (früher Arbeitsstand im Teilprojekt).

Auch für die Umsetzung der Gesamtmethode durch PROSTEP im Traceability-Demonstrator wurde zusätzlich im weiteren Verlauf auf die Ergebnisse des in Kapitel 3.1.2.9.4.1 beschriebenen Vorgehens des Prozesses zum projektinternen Baselining und der projektinternen Ergebnisfreigabe und Dokumentation zurückgegriffen. Das Vorgehen war in der frühen Phase des Projektes unter anderem auch darauf ausgelegt, die Durchgängigkeit und Traceability der Entwicklungsartefakte entlang der Prozesskette sicherzustellen und diente als ein Kernelement für die Dissemination der Projektergebnisse für den Halbzeitevent.

Die von den Projektpartnern zur Verfügung gestellten Inhalte wurden für die Dokumentation der Methode in verschiedene ineinandergreifende Prozesse und Subprozesse untergliedert und mit konkreten Entwicklungsartefakten angereichert. Abbildung 280 zeigt einen Ausschnitt aus der auf dem Halbzeitevent vorgestellten Dokumentation der Methode. Im Übersichtsbaum links sind bereits die Grundbausteine des späteren „Development & Operations – Global“ (vgl. Abbildung 270 und Abbildung 271), sowie Elemente der tieferen Ebenen, zum Beispiel „Specification of Target behavior“, Test Orchestration“ oder „Test Execution“, zu erkennen.

Auch in dieser Darstellung wurde bereits soweit vorhanden, der Prozessfluss, erkennbar an den blauen Pfeilen in der Abbildung, mit modelliert. Der innere Aufbau der einzelnen Aktivitäten konnte in dieser Phase des Projektes noch nicht vollständig und durchgängig für alle Elemente beschrieben werden. In dieser Darstellung wurden primär, auch in Hinblick des Showcases für das Halbzeitevent, konkrete Arbeitsergebnisse des Projektes den jeweiligen Aktivitäten zugeordnet. Dies geschah, um diese im Gesamtzusammenhang des bis dahin definierten Assurance Frameworks einzuordnen und die Zusammenhänge zu visualisieren. Abbildung 280 (links) zeigt zum Beispiel, dass die „Formalisierung des PSM“, die „PSM-Software“, sowie das „Risk Assessment“ Teile der „Specification of Target Behavior“ sind.

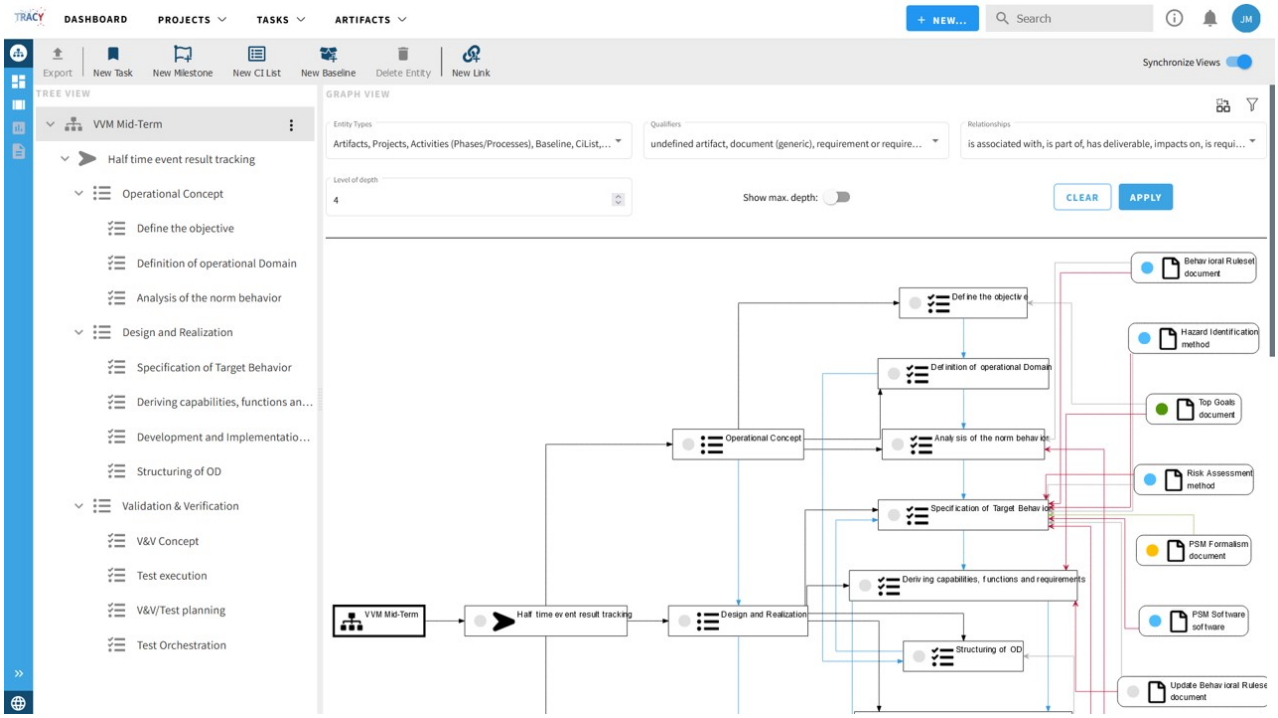


Abbildung 280: Ausschnitt aus der auf dem Halbzeitevent präsentierten Umsetzung in TRACY.

Für die Umsetzung des Traceability Demonstrators auf dem Halbzeitevent wurden durch PROSTEP speziell an das Event angepassten Funktionen implementiert. So wurden einerseits Elemente der graphischen Oberfläche überarbeitet und damit vereinfacht, um diese zu verschlanken und den Einstieg zu erleichtern, da bestimmte standardmäßig vorhandene Funktionalitäten für diese Darstellung nicht benötigt wurden. Zum anderen wurde eine Read-Only Funktionalität implementiert, um Änderungen an den Inhalten durch Dritte auf dem Event zu verhindern. Die konkreten Anpassungen am Tool wurden in TP1 von PROSTEP durchgeführt.

Für die finale Umsetzung im Traceability Demonstrator standen weniger die einzelnen konkreten Arbeitsergebnisse, wie im Halbzeitevent, im Vordergrund. Der Fokus lag auch hier, wie im SysML-Modell, auf der Darstellung und Dokumentation der Durchgängigkeit der VVM-Gesamtmethode. Aus diesem Grund wurde für die finale Umsetzung eine komplett neue Implementierung der Inhalte der VVM-Methode durchgeführt.

Die Strukturierung der Dokumentation orientiert sich hierbei ebenfalls an den vier Hauptebenen, „Development & Operation – Global“, „Development & Operation – Scenarios“, „Argumentation“ und „Risk Management“, der Gesamtmethode (vgl. Abbildung 277 und Abbildung 282 oben links). Innerhalb dieser Ebene wurde eine Dekomposition in die einzelnen, zur Ebene gehörigen Prozessschritte, durchgeführt. Es ergibt sich somit eine baumartige Top-Down-Struktur, die dokumentiert aus welchen Prozessschritten bestimmte Elemente der Methode bestehen und welche In- und Outputs sie besitzen. Abbildung 281 zeigt beispielhaft dazu, den inneren Aufbau des Synchronisationspunktes „Capability Identification Process“ mit den zugehörigen In- und Outputs.

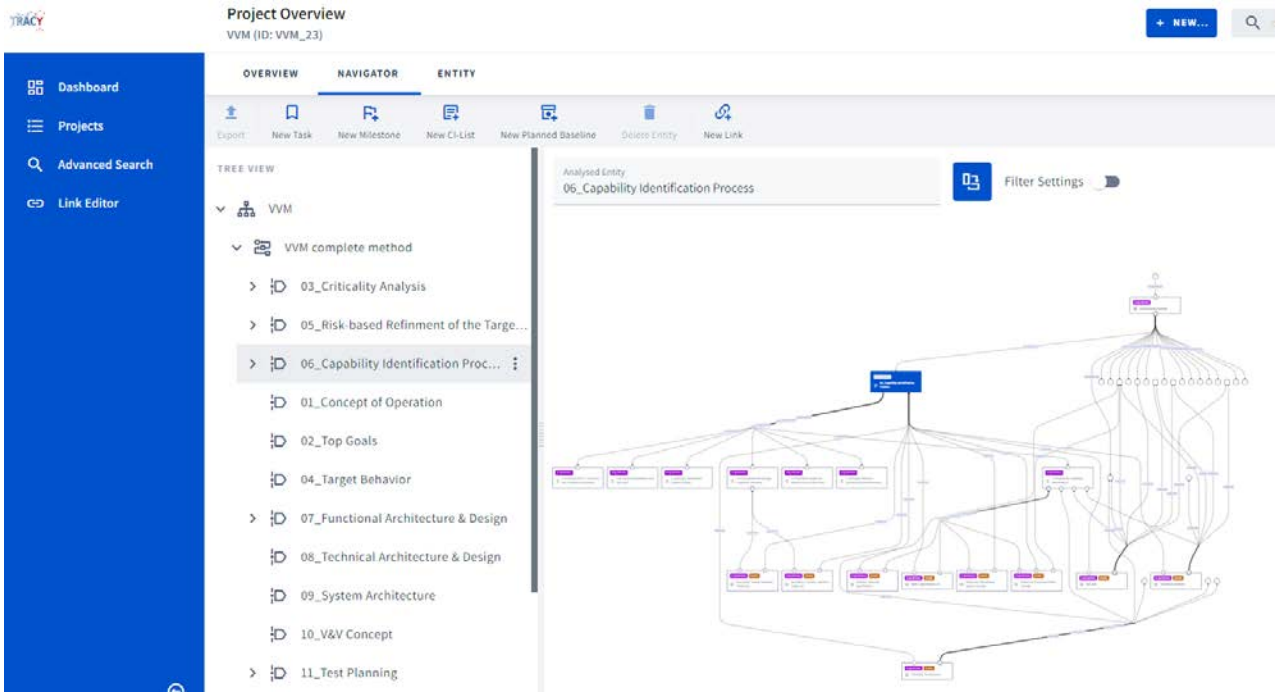


Abbildung 281: Aufbau des Synchronisationspunktes „Capability Identification Process“ in TRACY für das Abschlussevent (finaler Softwarestand).

TRACY bietet zusätzlich in der Benutzeroberfläche auswählbare Filterkriterien, basierend auf denen beispielsweise nur der Aufbau einzelnen Prozessschritte oder nur deren konkrete In- und Outputs angezeigt werden können. Zudem lässt sich auch Einstellen auf wie vielen Detaillierungsebenen dies angezeigt werden soll. Dies ermöglicht eine einfache Navigation durch die VVM-Gesamtmethode, um genau die Inhalte in der jeweils gewünschten Detaillierungstiefe angezeigt werden, die der Benutzer wünscht.

Abbildung 282, oben rechts zeigt den strukturellen Aufbau des Methodenelements „Test Planning“. Da alle anderen Abhängigkeiten durch den Filter entfernt wurden, entsteht eine übersichtliche Darstellung der einzelnen Subprozesse, aus denen das Methodenelement besteht. Unten links wurde eine Filterung auf die In- und Outputs durchgeführt. Es lässt sich anschaulich darstellen, welche Übergabeelemente von dem Subprozess „Identify Hazards“ erzeugt und/oder benötigt werden. Dies entspricht damit genau den Elementen auf den Außenkanten einer Aktivität im SysML-Modell. Des Weiteren bietet TRACY die Möglichkeit Impaktanalysen durchzuführen. Abbildung 282, unten rechts, zeigt dies exemplarisch für das Artefakt/ Übergabeobjekt „Hazard“. Die dargestellten Verbindungen zeigen alle Artefakte, die auf die Erzeugung des Objektes „Hazard“ einen Einfluss haben. Es sind also alle Artefakte aufgelistet, die im Gesamtmodell Eingangsgrößen in Prozesse sind, die „Hazard“ als Ausgangsobjekt haben. Auch die entgegengesetzte Darstellung, die beispielweise zeigt, worauf „Hazard“ einen Einfluss hat, ist als Funktion implementiert. Dies ermöglicht es, schnell zu identifizieren welche Elemente von Änderungen betroffen sein könnten.

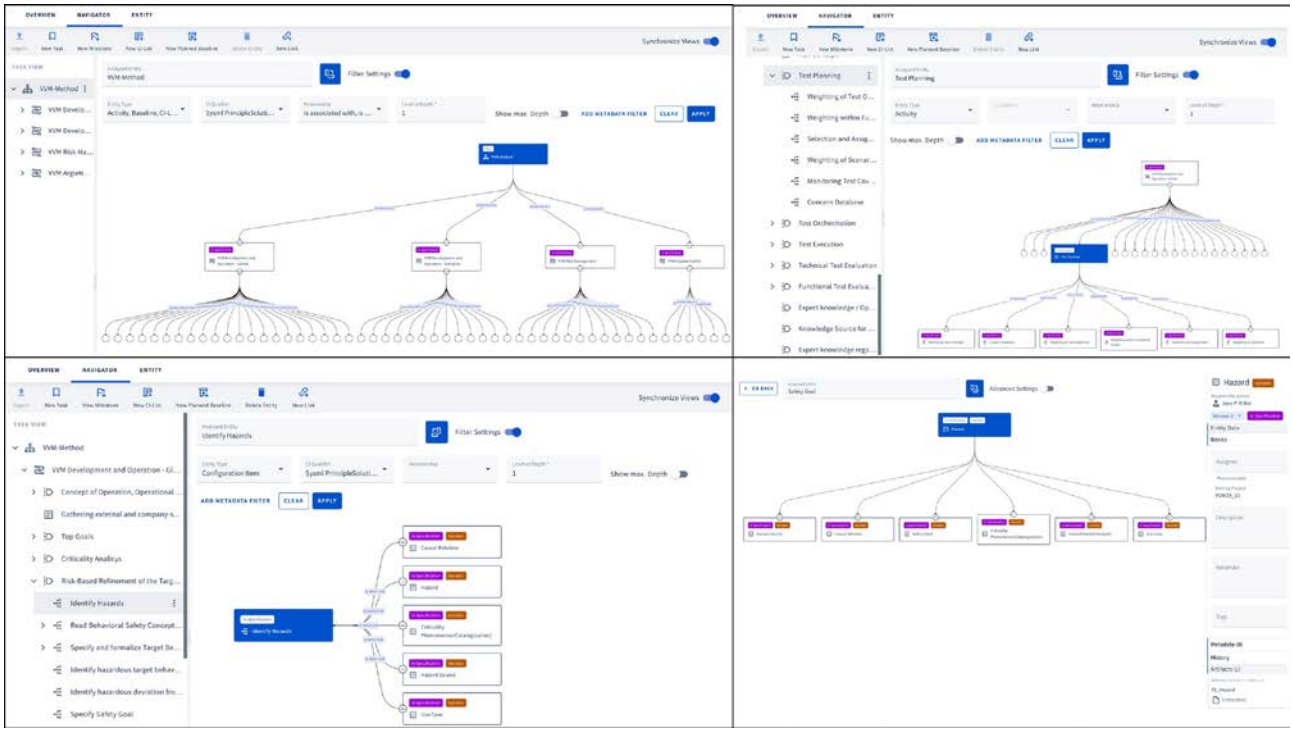


Abbildung 282: Übersicht verschiedener Darstellung und Filteroptionen in TRACY.

Die Implementierung in TRACY bietet somit eine sinnvolle Ergänzung zum SysML-Modell, da hier einzelne Zusammenhänge anders oder einfacher dargestellt werden, als dies im SysML-Modell möglich ist. Für ähnliche Darstellungen im SysML-Modell müsste zum Teil direkt die zur Modellierung verwendete Software genutzt oder neue Diagramme eingefügt werden, was in der HTML-Ausleitung nicht möglich ist.

3.1.2.9.6 Zusammenfassung und weiteres Vorgehen

Der vorliegende Abschnitt zum Teilprojekt 9 beschreibt die Inhalte der Anforderungserhebung, die Zusammenarbeit mit TPX, die Etablierung des projektinternen Baselinings und das Vorgehen und die Ergebnisse der Dokumentation der VVM-Gesamtmethode in SysML und im Traceability Demonstrator. Beide Dokumentationsmethoden unterstützen dabei die industrielle Instanziierbarkeit der VVM-Projektergebnisse durch die ihnen zugrundeliegende konsistente und durchgängige Beschreibung der Methode. Zusätzlich unterstützt die Dokumentation die Dissemination der Projektergebnisse und den Austausch mit projektfremden, externen Experten, da sie einerseits durch die formale, domänenunabhängige Beschreibung eine einheitliche Diskussionsbasis schafft und zum anderen durch die graphische Repräsentation und den Top-Down-Ansatz mit unterschiedlichen Granularitätsebenen einen leichten Einstieg in die VVM-Gesamtmethode schafft.

Die VVM-Gesamtmethode wurde zu diesem Zweck in miteinander in Beziehung stehende Aktivitäten zerlegt und in dieser Form dokumentiert. Zudem sind zu den einzelnen Aktivitäten die Übergabe- und Austauschobjekte konsistent über die gesamte Methode beschrieben. Somit dienen sie als „roter Faden“ entlang der Prozesskette und stellen die einzelnen Verbindungen zwischen den Elementen der Methode her.

In enger Zusammenarbeit mit den VVMethoden-Projektpartnern wurde damit ein Instrument geschaffen, in Form des SysML-Modells und der Abbildung der Methode im PROSTEP-

Traceability Demonstrator, dass die Zugänglichkeit und Nachvollziehbarkeit der VVM-Gesamtmethode auch über die Projektgrenzen hinaus nachhaltig unterstützt. Es unterstützt dabei auch die folgenden Punkte:

- Informationen domänenübergreifend verknüpfen und nachverfolgen.
- Projekte gemäß den Top-Prozess.Anforderungen steuern.
- Mit Partnern zusammenarbeiten.
- Sicherstellung der Konsistenz durch formalisierte Beschreibung.
- Einen digitalen Faden aufbauen.
- Analysieren von Auswirkungen.
- Eine grafische Darstellung der VVM-Methode bereitstellen.
- Erstellung einer navigierbaren "Blaupause" für die industrielle Anwendung der VVM-Methode.

Die Ergebnisse der Dokumentation wurden nach Projektende den Partnern auf unterschiedliche Arten, sowohl im Proprietärformat als auch in nichtproprietären Formaten zur weiteren Verwendung in den Häusern zur Verfügung gestellt. Darüber hinaus ist der finale Stand der SysML-Dokumentation als HTML-Export auf der VVM-Homepage für die Öffentlichkeit zugänglich gemacht worden, um den oben beschriebenen Austausch mit Experten und Interessierten aktiv voranzutreiben.

3.1.2.10 TPX

3.1.2.10.1 Executive Summary Abschlussbericht Teilprojekt VVM-TPX

Der nachfolgende Bericht fasst Ergebnisse und weitere wichtige Informationen aus den durch das VVM-Teilprojekt TPX geleiteten Aktivitäten zur internationalen Vernetzung, operativen Kollaboration und Ergebnisverbreitung der Projekte VVM und SET Level mit weltweit aktiven Initiativen zum szenarienbasierten Sicherheitsnachweis zusammen. An der Durchführung des Teilprojektes VVM-TPX sowie der Erarbeitung der Ergebnisse waren sowohl die VVM Projektmitglieder beteiligt als auch projektexterne Gruppierungen auf freiwilliger Basis. Stets wurden im TPX Kontext die Projekte SET Level und VVM unter der Bezeichnung „Projekt der PEGASUS Projektfamilie“ geführt um sowohl die auf PEGASUS basierende Grundmethodik beider Projekte als auch das weltweit durch PEGASUS eingeführte Interessentennetzwerk aktiv fortzuführen.

Ausgangspunkt für alle Vernetzungs- und Kollaborationsaktivitäten war der in 2019 durch das PEGASUS Projekt (https://www.pegasusprojekt.de/de/) erarbeitete methodische Sicherheitsnachweis und dessen Prozessschritte und Spezifikationen sowie die aus dem PEGASUS Netzwerk stammenden Liaisons und Interessentennetzwerke.

3.1.2.10.1.1 Management Zusammenfassung

Szenarienbasierte Prüfmethoden zum Nachweis der Sicherheit von ADS, der damit verbundene Bedarf an Prozessschritten für Test und Entwicklung im Rahmen einer Gesamtmethodik sowie zusätzlich kohärente Messwerte, Formate, Testverfahren und Parameterbereichen sowie die notwendige Verlagerung des Prüfraums in Simulationsumgebungen (oder virtuelle Umgebungen)

standen und stehen noch immer im Mittelpunkt vieler globaler Forschungs- und Entwicklungsinitiativen. Die Motivation der meisten dieser Initiativen besteht in dem Bestreben nach der notwendigen Reduzierung des beim automatischen Fahrens perspektivisch unbegrenzten Parameterraums im Zusammenhang mit den Herausforderungen der Entwicklung, Prüfung und Typenzulassung einer ADS-Funktionalität (ADS = Automated Driving System).

Diese Initiativen müssen sich neben der wissenschaftlich getriebenen und mit Instrumenten der Ingenieurswissenschaften umgesetzten Entwicklung der Methodiken auch den Vorgaben aus Regulierung und aus der Standardisierung stellen, die sich zur Projektlaufzeit in verschiedenen Entwicklungsstadien befanden und fortwährend weiterentwickelt werden.

Aus diesen Gründen hat VVM-TPX begleitend zu der projektinternen Entwicklung der VVM Gesamtmethode operative Systematiken entwickelt, nach denen der Informationsfluss sowohl zu den weltweiten Gruppierungen, zu den Standardisierungsgruppen als auch zu den regulierungsnahen Gremien etabliert werden konnte.

Die wichtigsten dieser Gruppierungen und die jeweilige aktive Rolle von VVM zu diesen sind im Folgenden genannt

Regulierungsnahe Gremien, u.a. die unter der UN ECE WP29 „Weltforum für die Harmonisierung von Fahrzeugvorschriften“ geführten harmonisierenden Arbeitsgruppen VMAD (https://wiki.unece.org/pages/viewpage.action?pageId=60361611), GRVA (https://unece.org/transport/events/wp29grva-working-party-automatedautonomous-and-connected-vehicles-9th-session) und FRAV (https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction) oder auch das „EU Joint Research Center“ (JRC.C4 - https://joint-research-centre.ec.europa.eu/index_en) in Europa, bestreben vereinheitlichte Spezifikationen, Prozesse und Metriken zum szenarien- und simulationsbasierten Sicherheitsnachweis an. An diesen Gruppen der UN ECE WP29 wurden vorrangig an Sitzungen der Arbeitsgruppe VMAD teilgenommen und dort Teile der VVM Gesamtmethode zur Diskussion gebracht.

Auch in USA staatlich organisierte Gruppierungen zur Harmonisierung des Sicherheitsnachweises und von Testmethoden und -szenarien, z.B. das US Department of Transport (DOT), dessen Themenbereiche von privaten Initiativen flankiert werden war Gegenstand mehrerer fahclicher Diskussionen. Diese erfolgten z.B. im Rahmen von Workshops und auf Sessions z.B. am Rande von wichtigen Symposien (z.B. der annual TRB ARTS Conference, z.B. auf der https://trb.secure-platform.com/a/page/AutomatedRoadTransportationSymposium).

Ebenso wurde ein dauerhafter Austausch auf fachlicher Ebene mit japanischen Institutionen wie z.B. das Japanese Automobile Research Institute (JARI - https://www.jari.or.jp/en/) oder die Japan Automobile Manufacturers Association (JAMA - https://www.jama.or.jp/english/about/organization.html) durch TPX verstetigt. Die dort gemeinsam geführten Diskussionen fanden u.a. auf dem jährlichen SIP-adus Symposium statt, siehe z.B. https://en.sip-adus.go.jp/evt/workshop2022/ oder https://mobilityinnovationalliance.org/mobiweekjapan2023/en/, um dort Harmonisierungsbestrebungen zu szenarienbasierten Prüfmethoden zu diskutieren sowie gegenseitige Nutzungsszenarien aufzuarbeiten. VVM war auf allen SIP-adus Konferenzen mit Leadbeiträgen vertreten sowie über session leads der jeweiligen break-out sessions zur Safety Assurance. Die Kollaboration ist derzeit angestrebt fortgesetzt zu werden mit verstärktem Fokus

auf Einführung von Datenökosystemen in die Methodiken zum szenarienbasierten Sicherheitsnachweis.

Da alle diese Initiativen aus Forschung, Industrie, Testdesign, Normung und Regulierung ein gemeinsames Ziel nämlich die Entwicklung und Harmonisierung szenarienbasierter Entwicklungs- und Validierungsverfahren und die damit verbundene Verlagerung des Design- und Testraums in virtuelle Räume verfolgen wurden durch das Teilprojekt VVM-TPX zu Projektbeginn an Vernetzung und Liaisons mit Akteuren aus diesen Gruppierungen aufgebaut, um kontinuierlich Diskussionen zwischen VVM mit diesen Initiativen zur beidseitigen Nutzung/Harmonisierung der Methoden zu führen.

Zusätzlich waren und sind etliche privat organisierte Projekte, Initiativen und Gruppierungen mit Aktivitäten zu dem Themenkomplex tätig was ebenfalls zur Aufnahme dieser Projekte in das VVM Netzwerk führte. Dazu zählten unter anderem die Projekte HEADSTART (EU) und SUNRISE (EU), SAKURA (JP), die Projekte der VDA-LI (GE) https://www.vda.de/de/themen/digitalisierung/Autonomes-und-vernetztes-Fahren sowie die Szenarien-DB Initiativen von ADScene (FR), WMG Warwick (UK) und GAIA-X 4 Future Mobility (GE). Der Abgleich mit diesen Projekten/Initiativen erfolgte stets in einer mit dem Projekt SET Level gemeinsam abgestimmten Vorgehensweise.

Zusätzlich waren auf Seite weltweiter Standardisierungsaktivitäten z.B. aus ISO und ASAM aber auch weiterer Gruppierungen mehrere Stränge zur Harmonisierung gestartet oder weitergeführt worden. Auch mit diesen Standardisierungsgruppierungen wurden teilweise intensive bidirektionale Gespräche geführt um einen gemeinsamen Abgleich der jeweiligen Interessen zu erzielen.

Als zusätzliches Element zur systematischen Vernetzung der VVM Gesamtmethode sowie der VVM Projektmitglieder mit externen Stakeholdern wurden die beiden wichtigsten Disseminationsevents von VVM, das Halbzeitevent und das Abschlussevent genutzt um am jeweiligen Folgetag ein Austauschsymposium zur internationalen Kollaboration mit den wichtigsten internationalen Akteuren zu führen. Ziel war sowohl das Zusammenführen der aktuellen Wissensstände von mit VVM vergleichbaren Initiativen und Projekten auf einer durch VVM organisierten Bühne sowie das gemeinsame Diskutieren über aktuelle und weitere Herausforderungen beim szenarienbasierten Sicherheitsnachweis. Aus diesen beiden Symposien gehen zahlreiche Statements zum Status der Forschung und Umsetzung hervor, siehe Material unter

- VVM Halbzeitevent 2022: https://www.vvm-projekt.de/midterm-docs
- VVM Abschlussevent 2023: https://www.vvm-projekt.de/virtual-fe-exhibition

Als weiteres elementares symposienartiges Austauschformat wurde die in PEGASUS etablierte Reihe der internationalen PEGASUS Expert Workshops (PEW) fortgeführt. Dabei wurden zur Unterstützenden Definition der VVM Grundthesen der PEW#7 „Automated Driving - Building a robust Safety Case“ in 2020 sowie der PEW#8 „Formalizing the Safety Case“ in 2022 durchgeführt.

Aus beiden PEWs gingen international harmonisierte Grundfragen und Lösungsansätze hervor die im weiteren Verlauf dieses Berichts zusammengefasst sind.

3.1.2.10.1.2 Operationalisierung von VVM-TPX

Für das Projekt VVMethoden (https://www.vvm-projekt.de/en/) wurden von VVM-TPX stets das Angebot an die Kooperationspartner formuliert grundlegende und skalierbare Ansätze für eine umfassende Gesamtmethodik zur szenariobasierten Sicherheitsverifikation und -validierung beim automatisierten Fahren zu entwickeln und dies in Bereitschaft zur Harmonisierung mit den Methoden der Kollaborationspartner zu diskutieren. Diese Aktivitäten erfolgten stets in Kombination mit dem Projekt SET Level (https://setlevel.de/) welches als Teil der PEGASUS Projektfamilie mit einer projektübergreifenden Argumentationsstruktur für die Sicherheitsverifikation und -validierung von ADS unter Verwendung von Entwurfs- und Implementierungsmethoden szenariobasierter Ansätze aufwartet.

Da Arbeiten in den Projekten VVM und SET Level von Projektbeginn an in Interaktion mit weltweiten Partnerinitiativen und -projekten sowie Standardisierungsgremien durch Kooperation und gemeinsame Expertenworkshops der PEGASUS-Familie durchgeführt wurden wurde mit dem Label „Project of the PEGASUS Family“ ein inoffizielles Identifizierungsmerkmal auch für die Partner eingerichtet, so dass die vorstehend genannten Liaisonaktivitäten und Harmonisierungs eine Grundlage und Projektionsfläche für gemeinsam erarbeitete Fragestellungen und Lösungskorridore hatten.

Die für diesen Abschlußbericht relevanten Ergebnisse werden in den folgenden Kapiteln dargelegt. Es handelt sich dabei im Wesentlichen um gesammelte Ergebnisse aus Mitschriften und Protokollen der gemeinsam mit unterschiedlichen Partnern geführten offenen Fachdiskussionen. Eine tragende Säule spielen dabei vor allem die bereits erwähnten PEGASUS Expert Workshops die mit bis zu 200 Teilnehmern aus bis zu 11 Ländern im Zeitraum 2019 – 2023 durchgeführt wurden, aus mehreren deutsch-japanischen Symposien sowie Einzelabstimmungen (z.B. aus der SIP-adus Reihe). Zusätzlich erfolgte dies aus etlichen bilateralen Gesprächen mit den in Kap. 1.1 genannten Initiativen sowie mittels offener VVM-TPX sessions auf den ITS World und ITS World und ITS Europe Konferenzen 2021 und 2023 sowie auf den TRB ARTS Konferenzen in USA.

Ein weiteres wichtiges VVM-TPX Element war die Gestaltung internationaler Cooperation Days am Rande des VVM Halbzeitevents sowie des VMM Abschlußevents aus denen zusätzliche Impulse und Abgleichsszenarien hervorgingen.

3.1.2.10.2 2 Ergebnisse der Arbeitsgruppen von VVM-TPX

3.1.2.10.2.1 Flankierende Aktivitäten aus Regulierung und Relation zu VVM

Im Folgenden ist die TPX Analyse der Berichte und Diskussionen aus den relevanten Arbeitsgruppen der UN ECE WP29 zusammengefasst.

Die UN ECE WP 29 (https://unece.org/wp29-introduction) ist eine Arbeitsgruppe die sich der Aufgabe der Erschaffung eines einheitlichen Regelsystems für den Fahrzeugbau gestellt hat um die internationale Harmonisierung u.a. rund um das Thema Homologation zu erleichtern. Sie besteht aus weiteren Arbeitsgruppen (siehe Abbildung 283), die sich mit verschiedenen Themen der Harmonisierung im Fahrzeugbau beschäftigen.

Die Arbeitsgruppe Working Party on Automated/Autonomous and Connected Vehicles (GRVA - (https://unece.org/transport/events/wp29grva-working-party-automatedautonomous-and-connected-vehicles-9th-session) ist dabei verantwortlich für die Sicherheit von automatisierten Fahrassistenzsystemen und vernetzter Fahrzeuge. Dazu wurden weitere informelle

Arbeitsgruppen (IWGs) für verschiedene Themengebiete erstellt. Hier zu erwähnen sind die Gruppen VMAD und Functional Requirements for Automated Vehicles (FRAV - (https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction), da diese beiden Gruppen aufeinander aufbauen. Die FRAV erarbeitet die funktionalen Anforderungen der automatisierten Fahrzeuge und Fahrassistenzsysteme und die VMAD (https://wiki.unece.org/pages/viewpage.action?pageId=60361611) die entsprechende Absicherung dieser Systeme.

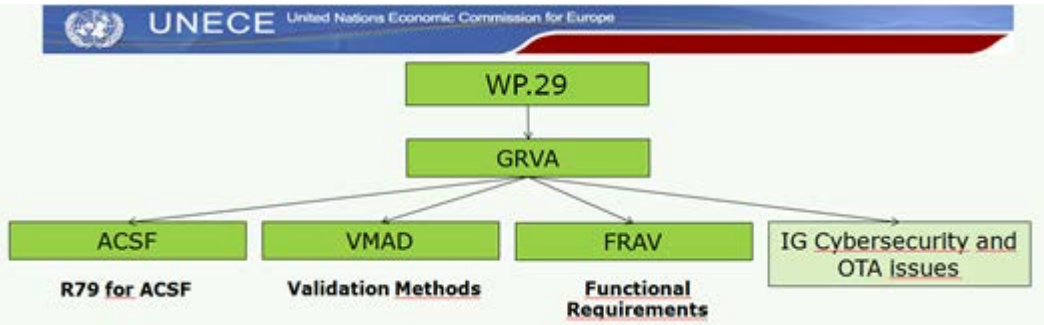


Abbildung 283: Struktur der WP.29 und GRVA.

Das Ziel des NATM Dokuments ist die Entwicklung einer Methode zur Validierung automatisierter Fahrsysteme, dabei muss diese wiederholbar, objektiv und evidenzbasiert sein. Um die Innovation der Automobilindustrie zu ermöglichen, soll die Methodik auch techonologieneutral und flexibel sein. Weiterhin gibt das Dokument einen Überblick über einen Szenarienkatalog mit Szenarien, die bei der Validierung beachtet werden müssen und einen Überblick über jede Säule des Multi-Säulen Ansatzes. Diese Punkte werden zusammengeführt und es wird dargestellt, wie diese Aspekte zusammenarbeiten, um einen effizienten, verständlichen und kohäsiven Prozess zu erlangen.

Von besonderer Relevanz für VVM war dabei das aus VMAD entwickelte leitende Dokuments „NATM“ (New assessment/test method for automated driving) welches am 13.04.2021 emittiert wurde (https://unece.org/sites/default/files/2021-04/ECE-TRANS-WP29-2021-61e.pdf) und auch für den Abgleich mit der VVM Gesamtmethode genutzt wurde.

Die Struktur der dort beschriebenen Prozesse entspricht einem Multi-Säulen Ansatz (siehe Abbildung 284). Die Säulen bestehen hier aus Simulation/virtuellem Testen, Testen auf dem Prüfgelände, Testen auf öffentlichen Straßen und dem Auditprozess. Die ersteren drei Säulen sind die Testmethoden und die letzte der Prozess, der mithilfe der Testmethoden die Sicherheit des Systems validiert. Die Säulen wurden mit Szenarienkatalogen ergänzt, um das Testen der Systeme mit den unterschiedlichen Säulen effizient, objektiv und skalierbar zu ermöglichen. Zusammen sollen die Säulen mit dem szenarienbasierten Testen die hoch komplexe Aufgabe der Validierung meistern.

Die Ansätze dieser Struktur ähneln denen von VVM, z.B. durch das V-Model in welchem der rechte Ast für die Prüfung des Systems, mittels Simulation, Teststrecke und öffentlichen Verkehr, zuständig ist. Zum Testen wird hier auch der szenarienbasierte Ansatz gewählt. Somit besteht eine grundsätzliche Kompatibilität zwischen VVM und den Ergebnissen von VMAD Der linke Ast des V-Models ist für die Anforderungsanalyse des Projektes zuständig und kann somit mit der Arbeit der

FRAV Gruppe verglichen werden, wo die funktionalen Anforderungen der Fahrassistenzsysteme und automatisierten Fahrzeuge erarbeitet werden.

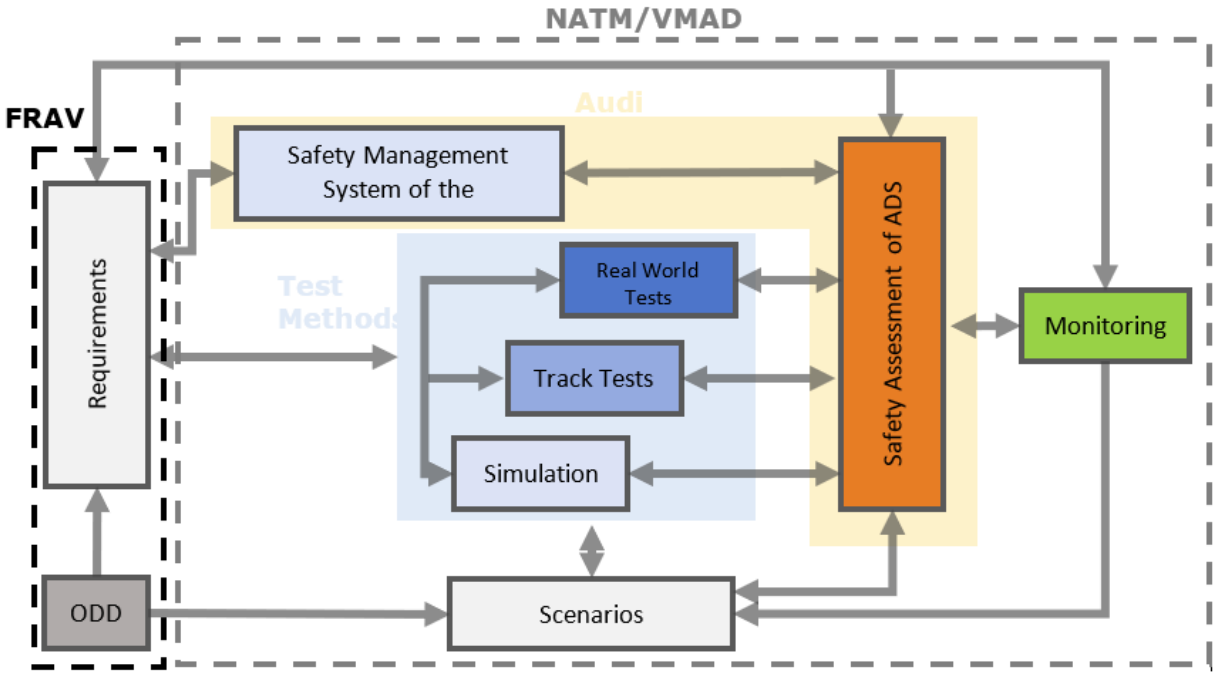


Abbildung 284: Struktur der Prozesse des Masterdokuments NATM aus VMAD und der FRAV.

Ebenso teilt NATM die Vorgabe mit VVM, dass die Validierung wiederholbar, objektiv und evidenzbasiert ist und Szenarien für das Testen so gewählt werden sollen, dass die geforderten Anforderungen erfüllt werden können. Damit ermöglicht der szenarienbasierte Ansatz eine vollständige Abdeckung der Verkehrsszenarien. Ein Verkehrsszenario laut VMAD ist eine Sequenz oder Kombination von Situationen, die genutzt werden, um die funktionalen Anforderungen der ADS zu bewerten. Außerdem können Szenarien auf alle 3 Testsäulen angewendet werden, um deren Stärken entsprechend auszunutzen. Die VMAD sieht hier allgemein vor, mit Szenarienkatalogen aus relevanten Szenarien zu erstellen, verbleibt jedoch unscharf was die Realisierung angeht. Hier liefert VVM eine anwendbare Antwort.

Da laut NATM die szenarienbasierten Validierungsmethoden eine adäquate Repräsentation von relevanten, kritischen und komplexen Szenarien enthalten müssen, fordert NATM komplexe Prozesse zur Vielzahl der Möglichkeiten diese Szenarien zu identifizieren. Dazu gehören das Analysieren von menschlichem Fahrverhalten, von Kollisionsdaten, von Verkehrsmustern in bestimmten ODDs und von gewonnenen Daten von ADS Sensoren. Zusätzlich spielen aufgezeichnete, feingranulare Verkehrsdaten z.B. über Messfahrzeuge, Infrastrukturaufzeichnungen und Drohnenmessungen eine Rolle zum Erheben von formal testbaren Szenarien. Hier liefert VVM entsprechende Ansätze und Anwendungsbeispiele zur Kategorisierung. Ebenso sollen laut NATM Wissen und Erfahrungen, die bei der Entwicklung von ADS Systemen gesammelt wurden, synthetisch generierte Szenarien mit Variation von Schlüsselparametern und entwickelte Szenarien basierend auf funktionalen Sicherheitsanforderungen und der SOTIF, genutzt werden.

Um Szenarien zu Klassifizieren und deren Eigenschaften zu beschreiben wurden aus dem PEGASUS Projekt die Definition von funktionalen, logischen und konkreten Szenarien und das 6-Layer-Modell sowohl in NATNM als auch in VVM übernommen.

Die Testsäulen laut VMAD bestehen aus Simulation/virtuellem Testen und dem Testen auf Prüfgelände und auf öffentlichen Straßen. Die Säulen wurden so gewählt, da das Zusammenspiel aller Säulen es ermöglicht sich auf die Stärken jeder Säule zu fokussieren. Dadurch ist die Bewertung auf unterschiedlichen Stufen der Wahrheitstreue und Skalierbarkeit möglich. Beispielsweise erlaubt das Testen auf öffentlichen Straßen eine hohe Wahrheitstreue der Umgebung, jedoch können diese Tests kosten-, zeitintensiv und schwierig zu reproduzieren sein. Außerdem kann diese Testmethode ein Sicherheitsrisiko für andere Verkehrsteilnehmer darstellen. Das Testen auf dem Prüfgelände ist besser geeignet für Szenarien mit höherem Risiko, da hier andere Verkehrsteilnehmer nicht gefährdet werden können und die Reproduzierbarkeit vereinfacht ist. Als problematisch sieht NATM unterschiedliche Stör-Elemente wie z.B. Regen und Nebel in das Szenario einzufügen.

Simulationen sind skalierbarer, kosteneffizienter, sicher und effizienter im Vergleich zu den anderen beiden Testmethoden, können aber einen geringere Wahrheitstreue aufweisen und sich in der Qualität unterscheiden. Außerdem kann es schwierig sein Tests auf unterschiedlichen Plattformen zu reproduzieren. Der Auditprozess ist am besten dafür geeignet die gesamte Sicherheit eines ADS Systems zu testen, da Informationen wie Safety-by-design bestätigt werden und eine Analyse der Felddaten vom Hersteller enthält. Je nach Anforderung des Testszenarios können unterschiedliche Testmethoden angewendet werden und die Sequenz und Komposition der Säulen kann variieren.

NATM stellt klar, dass untersucht werden muss wie Behörden eine validierte und standardisierte Simulationsumgebung erhalten können, in der Hersteller das zu prüfende System mit einem „plug“-in Verfahren auf Einhaltung prüfen können. Da eine solche Standardisierung Thema von aktueller Forschung ist, sollen Simulations Toolchains von Herstellern erlaubt werden, sofern diese dokumentiert sind und erklärt werden können. Dafür sollen die Dokumentation und die entsprechenden Daten harmonisiert werden. Hier leistet VVM einen wesentlichen Beitrag um Prüfinstitutionen und -Behörden mit empfohlenen Vorgehensweisen und Verweis auf gültige oder bewährte Dokumente zu versorgen.

Die von VMAD gestellten und im NATM Dokument formulierten Empfehlungen/Forderungen an das Durchführen eines Sicherheitsnachweises wurden in der Entwicklungsphase von VVM berücksichtigt und im Rahmen der VVM Gesamtmethode detaillierter und mit weiteren Umsetzungsempfehlungen behandelt.

Ein weiteres in NATNM behandelter Aspekt ist das In-Use-Monitoring des ADS im Betrieb welches von VMAD aber nicht als Säule des Multi-Säulen Ansatzes betrachtet wird. Das In-Use-Monitoring soll für die Sicherheitsbestätigung, die Szenariogenerierung und Sicherheitsempfehlungen zuständig sein. Die Sicherheitsbestätigung erfolgt nach Markteinführung und bestätigt die initiale Bewertung der Auditphase. Die Szenariogenerierung erweitert die allgemeine Szenariendatenbank mit neuen und wichtigen ggfs. unbekannten Szenarien. Die Sicherheitsempfehlung kann abgeleitet werden aus dem Teilen und Lernen von Schlüsselunfällen. Analysen der Hersteller von aufgenommenen Daten sollen an Behörden mit Sicherheitsempfehlungen übergeben werden. In VVM wurde dieses Thema VHB-konform nicht behandelt, aber als Empfehlung für künftige, homologationsbegleitende Tätigkeiten formuliert.

Die zuletzt in Kraft gesetzten Vorgaben aus der Regulierung setzen erstmalig in Europa ein gesetzlich verbindliches Rahmenwerk zum Zulassungsverfahren für automatische Fahrfunktionen im größeren Maßstab vor. Da diese während ihrer Entstehung inhaltliche Bezüge zu den

genannten UN ECE WP29 Arbeitsgruppen hatten und zusätzlich auch in Teilen die Methodik des szenarienbasierten Testens aus PEGASUS verwendet wurde steht mit der VVM Gesamtmethode nun ein aus wissenschaftlicher Sicht die Regulierung ergänzendes methodische Werk zur Verfügung mit welchem Prozessschritte zum regelkonformen Nachweis von Sicherheit empfohlen werden und genutzt werden können.

Die derzeit gültigen Gesetzesvorschriften sind:

- Für Deutschland die AFGBV vom 04.06.2022: https://www.gesetze-im-internet.de/afgbv/AFGBV.pdf
- Für Europa die Implementing Regulation (EU) 2022/1426 vom 5 August 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1426
- Das ergänzende Dokument von EU JRC von 03/2024, „Update EU: Interpretation of EU Regulation 2022/1426 on the Type Approval of Automated Driving Systems“: https://publications.jrc.ec.europa.eu/repository/handle/JRC136417

3.1.2.10.2.2 Relation VVM zu den wichtigsten Standardisierungsaktivitäten

VVMethoden strebte im Rahmen seiner Austausch- und Verbreitungsaktivitäten an, einen systematischen Austausch mit wesentlichen Standardisierungsaktivitäten für die VVM Projektergebnisse zu schaffen, die VVM-Positionen in den Normen und Standards zu manifestieren und auch um dort wo geboten, die VVM- Gesamtmethode konform zu den aktuellen oder kommenden Standard- und Regelwerken auszurichten. Bei den für VVMethoden relevanten Normen- und Standardisierungsaktivitäten standen insbesondere die im folgenden aufgelisteten und in ihrer Verortung innerhalb des VVM Assurance Frameworks dargestellten im Fokus von VVM und waren sowohl Impulsgeber und Spezifikationsbasis als teilweise auch Gegenstand der VVM Liaison Aktivitäten.

Dabei war von Beginn an insbesondere die u.a. aus dem PEGASUS Projekt mit hervorgehende ISO Standardisierungsgruppe TC22 SC33 WG 34502 „Engineering Framework and processes of scenario-based evaluation“ die unter VVM Beteiligung fertiggestellt wurde von wichtiger Bedeutung für fachliche Ausrichtungen innerhalb VVM. Diese ISO Aktivität wurde begleitet von weiteren ISO TC22 SC 33 Working Groups deren Relation zu der VVM Gesamtmethode in Abbildung 3 dargestellt ist.

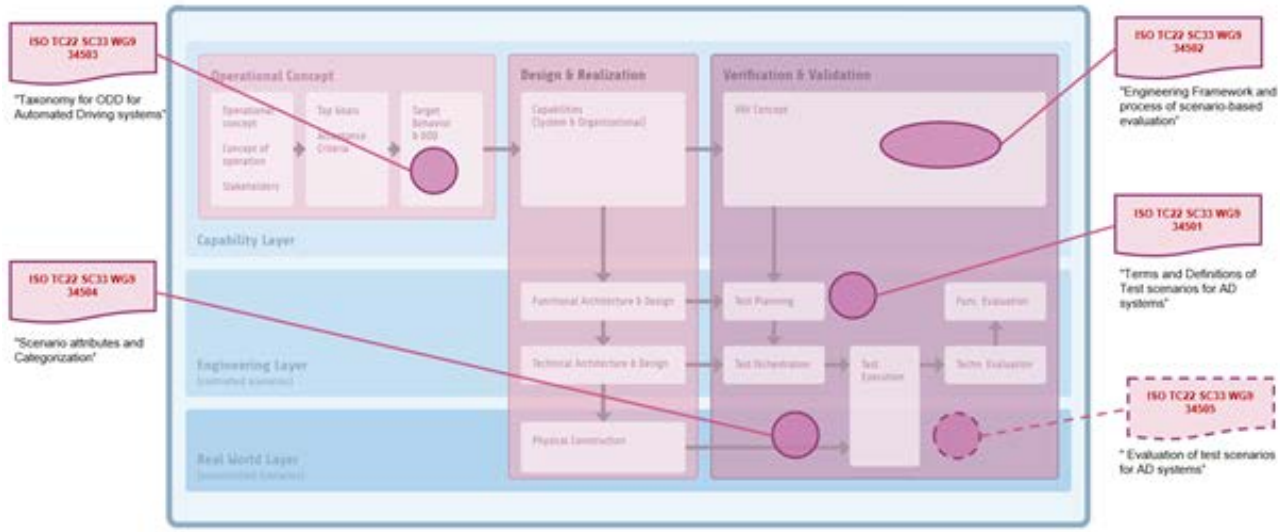


Abbildung 285: Verortung der ISO TC22 SC33 WG9 3450X Gruppen innerhalb des VVM Assurance Frameworks

Eine besondere Bedeutung als die VVM Gesamtmethode flankierendes Element kommt der für 2024 angekündigten Technical Specification Neue Aktivität ISO TC22 SC32 WG13 TS 5083 „Safety and cybersecurity for automated driving - Design, verification and validation" zu. Diese wird aus wesentlichen Vorgängerstandards hervorgehen (siehe Abbildung 286). Auch hier war VVM über wesentliche Akteure in den Arbeitsgruppen zur Definition des TS 5083 beteiligt.

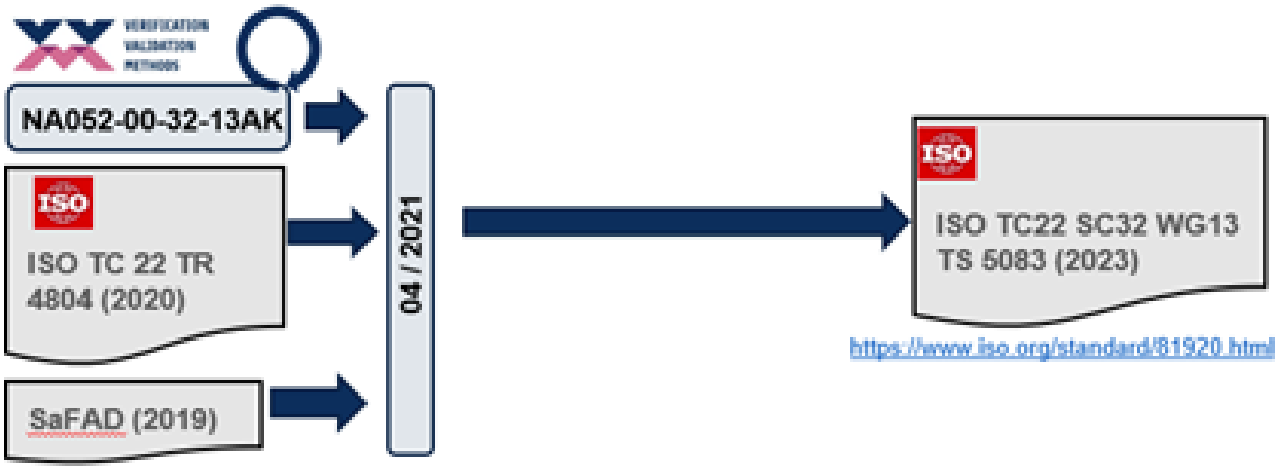


Abbildung 286: Entwicklungszusammenhang von zur ISO TC22 SC33 WG13 TS 5083

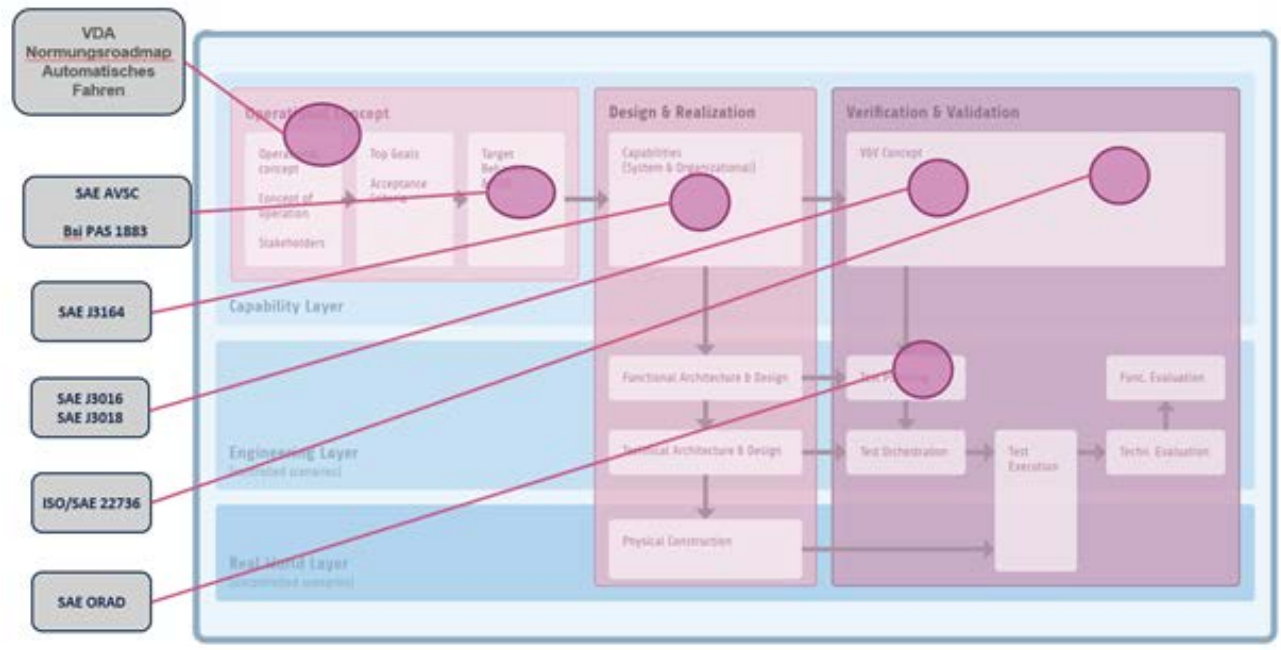


Abbildung 287: zeigt schließlich weitere Standardisierungsaktivitäten und deren Verortung im VVM Assurance Framework auf.

Weiterhin sind für die beispielhafte Umsetzung der VVM Gesamtmethode vor allem im Engineering Layer sind die in ASAM „Association for Standardization of Automation and Measuring Systems“ (https://www.asam.net/) entwickelten Standardisierungen auf technischer Ebene besonderer Bedeutung für. Dabei vor allem die ASAM Standards der ASAM Open.X Familie wie z.B. OpenScenario, OpenSimInterface, OpenDRIVE, OpenXOntology, OpenODD, OpenLabel, OpenCRG.

3.1.2.10.2.3 Technische Herausforderungen und Ansätze aus den PEGASUS Expert Workshops

Abbildung 288: Entwicklungsgeschichte der PEGASUS Expert Workshops bis zum PEW#7 "Building a robust Safety Case"

Die Reihe der PEGASUS-Expertenworkshops wurde ursprünglich 2017 vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) als eine unabhängige und offene Netzwerkreihe zum

Expertenaustausch initiiert, um vorläufige und endgültige Ergebnisse des PEGASUS-Projekts (https://www.pegasusprojekt.de) zu diskutieren und Schlüsselthemen im Bereich der Sicherheitsargumentation für automatisiertes Fahren zu erörtern. Die Termine und Themenauswahl der PEGASUS Expert Workshops 2017 – 2020 sind in Abbildung 6 dargestellt.

Der PEW#7 mit dem Titel "Building a robust Safety Case" fand als virtueller Workshop im September 2020 unter Beteiligung von 200 Gästen aus insgesamt 11 Nationen statt. statt. Neben der damit erreichten Reaktivierung der bewährten PEGASUS-Expertengemeinschaft unter der neuen Projektlinie VVM und SET Level wurde zusätzlich eine Analyse des PEW#7 genutzt, um als Ergebnis der geführten Diskussionen eine Auswahl von wichtigen Forschungsthemen zu definieren. Diese sind in Abbildung 289 dargestellt und waren thematisch teilweise bereits von VVM zur Bearbeitung vorgesehen.

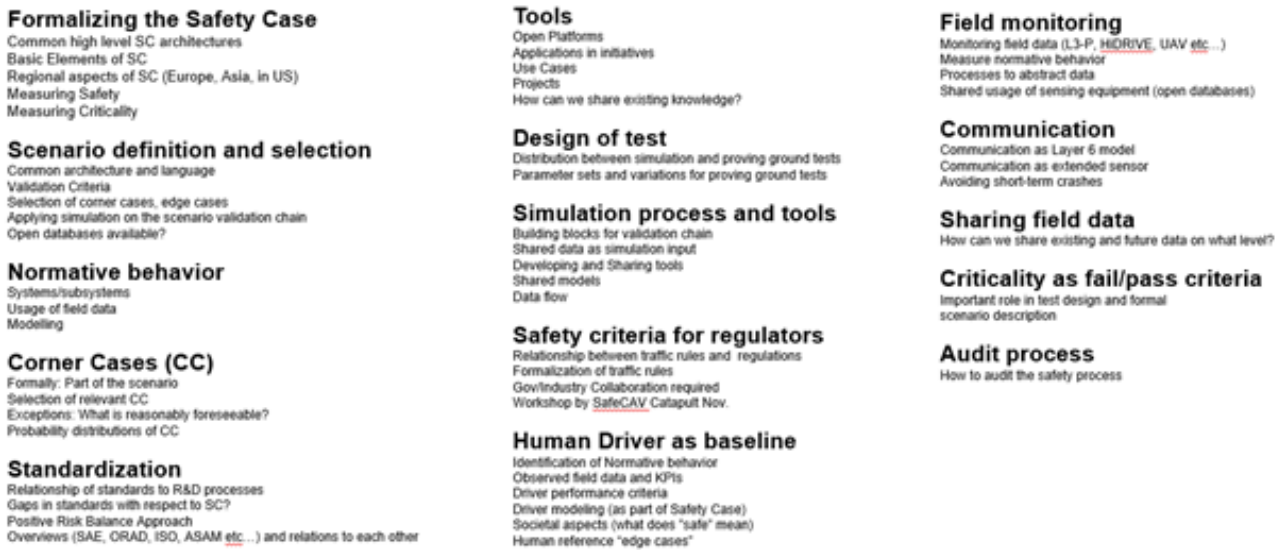


Abbildung 289: Key reserach topics aus der Analyse des PEW#7 "Building a robust Safety Case"

Diese Themenauswahl aus Abbildung 289 diente ebenso als Leitfaden für die folgenden thematischen Vorauswahlen der folgenden Expertenworkshops während der VVM Projektlaufzeit sowie als Wissenspool und zur Anregung neuer Initiativen. Aus diesen Themen wurde die Fragestellung „Was verstehen Sie unter "Formalisierung des Sicherheitsnachweises" und was sind die entsprechenden Grenzen und Hürden?“ als Motto für den PEW#8 herangezogen und diente damit gleichzeitig als Vorbereitung des internationalen PEGASUS Symposiums am zweiten Tag des VVM Halbzeitevents welches damit als weiterer Mulitplikator zur Vernetzung diente. VVM hat dort die folgenden VVM Hypothesen aufgestellt um anhand dieser die PEW Diskussionen zu moderieren und um daraus einen leitenden Rahmen für das internationale Symposium auf dem VVM Halbzeitevent abzuleiten.

Hypothese I: Beherrschung der Komplexität durch Abstraktion

- Analyse und Argumentation von Sicherheit z.B. durch eine Gefährdungs- und Risikoanalyse kann sicheres Verhalten eines Systems belegen
- Die Definition abstrakter Fähigkeiten kann sicheres Verhalten realisieren

Hypothese II: Messung der Sicherheit z.B. in Bezug auf die menschlichen Fähigkeiten

- Die Sicherheitsargumentation auf der abstrakten Verhaltensebene ermöglicht es, eine Behauptung in Bezug auf die Sicherheitsakzeptanzkriterien zu argumentieren

Hypothese III: Nachvollziehbare Dekomposition durch Argumentation

- Es kann davon ausgegangen werden, dass Fähigkeiten sicheres Verhalten abdecken, einschließlich Sicherheitsbelange, so dass die aus Fähigkeiten abgeleitete Zerlegung von Systemanforderungen für eine konsistente und nachvollziehbare Verifizierung und Validierung des Systems genutzt werden kann.

3.1.2.10.2.4 Herausforderungen an die Gesamtmethode

Die Entwicklung der VVM Gesamtmethode wurde begleitet von 6 durch TPX erarbeitenden leitenden Herausforderungen die auch über die Projektgrenzen hinaus bestand hatten, auch für zukünftige Aktivitäten rund um das szenariobasierte Testen. Diese können leitenden Charakter einnehmen z.B. für die Anwendung der VVM Gesamtmethode im konkreten Homologationsanwendungsfall, als thematische Korridore für Unternehmen die sich als Akteur im gesamten Sicherheitsnachweis positionieren wollen oder als Ideengeber für neue Projektinitiativen.

Dies Herausforderungen wurden u.a. auch stets in den durch TPX getriebenen internationalen Kollaboration eingebracht, um anhand ihrer eine Strukturierung möglicher Kooperationsthemen zu führen oder um und die Diskussionsthemen in Sessions zu führen.

Tabelle 10: Die Herausforderungen des Projektes

Herausforderung	Kurztitel	Lang
Herausforderung 1	**Definition von Sicherheit und sicheren Systemen im Straßenverkehr**	Die Gesellschaft erwartet gerechte Sicherheit, daher müssen die Sicherheit und die allgemeine Einhaltung der Vorschriften vor der Einführung gegenüber den Interessengruppen der Gesellschaft argumentiert werden. Das Nichtvorhandensein eines unangemessenen Risikos wird über verschiedene gesellschaftliche Forderungen - die Einhaltung von Gesetzen und Normen - argumentiert. Die Verwendung von quantifiziertem Risiko ist in dreifacher Hinsicht hilfreich: für die Festlegung von Auslegungswerten, für eine solide Sicherheitsargumentation und für nachvollziehbare Genehmigungsentscheidungen. Die Erwartung der Gesellschaft ist eine Sicherheitsargumentation mit Quantifizierung des Risikos. Die Erwartung der Gesellschaft ist eine Sicherheitsargumentation mit Risikoquantifizierung.

Herausforderung	Kurztitel	Lang
Herausforderung 2	**ODD-Zerlegung durch Szenarien und Argumentation der ODD-Abdeckung sind der Schlüssel zur Beherrschung des offenen Kontextes**	Die Argumentation einer repräsentativen ODD-Abdeckung durch spezifisch entworfene logische Szenarien ist der Schlüssel für eine systematische Kontrolle des Entwicklungs- und Validierungsraums (Hauptergebnis VVM), daher ist die Argumentation einer ausreichenden ODD-Abdeckung unter Verwendung des VVM ODD-Metamodells wesentlich für die gesamte VVM-Methode Das VVM ODD-Metamodell ist in diesem Sinne ein geeignetes und hinreichendes Modell der ODD, indem es eine strukturierte Methodik für die Realitätsabstraktion unter Verwendung unabhängiger logischer Szenarien mit speziellen Eigenschaften, den sogenannten Basisszenarien, einführt.
Herausforderung 3	**Sicherheitsargumentation und Entwicklungsprozess müssen übereinstimmen**	Sicherheitsargumentation und Entwicklungsprozess müssen auf allen Ebenen und in der gesamten Komplexität übereinstimmen. Um diese Komplexität zu beherrschen, sollten Argumentation, Design und V&V mit einer abstrakten Perspektive beginnen, d.h. unter Verwendung der Fähigkeiten und des Zielverhaltens des Systems, und von einer formalen Dekomposition gefolgt werden, um die Integrität und Sicherheit der Teilsysteme nachzuweisen. Legacy-Qualitätsprozesse müssen Metriken der formalen Dekomposition entlang der Argumentation berücksichtigen.
Herausforderung 4	**Virtualisierung ist obligatorisch**	Trotz aller systematischen Strukturierung stellt die Herausforderung für Systeme, die in einem offenen Kontext arbeiten, einen enormen Bedarf an Tests und Daten dar. Die Virtualisierung von Modellen und Daten auf allen relevanten Ebenen ist zwingend erforderlich. Natürlich gibt es noch eine beträchtliche Anzahl von Tests in der realen Welt, die abgeschlossen werden müssen.

Herausforderung	Kurztitel	Lang
Herausforderung 5	**Tools und Formate müssen kohärent sein und die Argumentation unterstützen**	Nahtlose Toolchains von der Simulation bis zum Proof-in-Field sollten auf offenen Spezifikationen und offenen (Daten)-Formaten basieren, d.h. Ontologien sollten ODD-Coverage unterstützen. Schnittstellen sollten Qualitätsmetriken von technischen Systemen und Teilsystemen unterstützen. Es sind gemeinsame Anstrengungen erforderlich, um standardisierte Formate und Metriken für die gesamte Toolchain einschließlich einer Proof-of-Concept-Implementierung zu entwickeln.
Herausforderung 6	**Die kontinuierliche Integration zwischen Verifikations- und Validierungsökosystemen muss ermöglicht werden.**	Datengetriebene Ansätze zur kontinuierlichen Einspeisung wachsender Daten- und Szenarienpools in industriell nutzbare und sich weiterentwickelnde Werkzeugketten sind ein wichtiger (und notwendiger) Erfolgsfaktor, um bestehende Sicherheitsfallketten mit zukünftigen Daten und angepassten Szenarien zu erweitern. Die Entwicklung und Anwendung qualifizierbarer, implementierbarer und zertifizierbarer Prozesse und Werkzeuge erfordert systematische Ansätze für die Zugänglichkeit und Interoperabilität, wie sie durch neue Ansätze in der Open-Data/Open-Source-Gemeinschaft entwickelt werden.

3.1.2.10.3 Ausblick auf thematische Zukunftsfelder über VVM hinaus

3.1.2.10.3.1 Szenariobasiertes Testen und Virtualisierung

Hochskalieren kritischer Szenarien

Selbst wenn die Annahme gerechtfertigt ist, dass es nur eine endliche und überschaubare Anzahl von sicherheitskritischen Faktoren zu berücksichtigen gibt, führt das Testen aller möglichen Kombinationen zu einer kombinatorischen Explosion, die jedes realistische Testbudget leicht übersteigt. Während das szenariobasierte Testen vielversprechende Ergebnisse liefert, werden die ODDs in der Praxis immer größer. In diesem Fall hängt die praktische Anwendbarkeit des szenariobasierten Testens direkt von der Fähigkeit ab, diese individuell unwahrscheinlichen, aber kollektiv relevanten Randfälle methodisch in die Sicherheitsfälle einzubeziehen. Wie können wir also effizient Nachweise für die Systemsicherheit in diesen Szenarien erbringen, z. B. in Form von Testdaten? Ein spezifischer Forschungsansatz, der sich der Generierung kritischer Szenarien widmet und Randfälle antizipiert, die den zunehmenden ODD-Raum abdecken, könnte eine

relevante und notwendige Antwort auf die Einführung des automatisierten Fahrens in größerem Maßstab sein.

Anwendung der ODD-Modellierung

Die Strukturierung der Operational Domain und der Operational Design Domain, wie sie von PEGASUS und VV Methods initiiert wurde, muss durch Beschreibungssprachen für die ODD erweitert werden, insbesondere für Simulationsanwendungen. Für viele Anwendungen des automatisierten Fahrens (L4) wäre es auch von großer Bedeutung, verbesserte On-Board-Algorithmen zur Verfügung zu haben, unabhängig davon, ob sich das Fahrzeug noch in seiner ODD befindet. Ansätze zur Verwendung von Kernszenarien für eine Datenbank mit sicheren Szenarien und die Kombination dieser "Atome" für größere ODDs, die aus gespeicherten Standardstücken zusammengestellt werden, müssen weiter untersucht werden, insbesondere für den Fall, dass die Kernszenarien nicht nur geometrische Beschreibungen wie "gerade Straße" oder "t-förmige Kreuzung" oder eine "Kreisverkehr"-Struktur abdecken. Dies ist besonders wichtig, wenn verkehrs- und/oder witterungsbedingte Effekte ins Spiel kommen, die den sicheren Betrieb eines ADS in einem bestimmten Verkehrsbereich, der unter Standardbedingungen als "sicher" gelten würde, beeinträchtigen könnten.

Realitätsabstraktion, virtuelle Umgebungen und entsprechendes Tooling

Für eine großflächige Anwendung der szenariobasierten Testmethodik VVM sind systematische Ansätze zur Übertragung der Realität in vielseitige virtuelle Elemente, wie z.B. Modelle, komplementäre Datensätze, die reale und virtuelle Daten mischen, sowie entsprechende und harmonisierte virtuelle Testeinrichtungen erforderlich. Während die derzeitigen Abstraktionsprozesse mehr oder weniger auf datengetriebener Realitätsabstraktion in ausgewählten Pilotprojekten beruhen, könnten neue (und skalierbare) modellbasierte Verfahren zur Kalibrierung und Validierung der Modelle den nächsten Schritt bei der Anwendung szenariobasierter Testmethoden in der Industrie einleiten.

Virtuelle Umgebungen spielen eine entscheidende Rolle bei der Verifizierung und Validierung (V&V), insbesondere wenn man Simulation als Dienstleistung betrachtet. Die effektive Integration verschiedener Testeinrichtungen und -umgebungen, wie virtuelle Umgebungen, Hardware-in-the-Loop (HiL)/Vehicle-in-the-Loop (ViL), Testgelände und Feldtests, ist für die Sammlung umfassender Beweise unerlässlich.

Innovative Daten- und Datendienst-Ökosysteme

Virtuelle Sicherheitsgarantien, die qualitativ hochwertige und nachvollziehbare Daten und Datendienste (teilweise basierend auf offenen Daten, synthetischen (KI-basierten) Daten, abstrakten Test- und Pilotstandortelementen) mit industriellen F&E- und V&V-Prozessen verknüpfen, sind erforderlich, um alle Anforderungen von Sicherheitsnachweis-Methodologien zu erfüllen. Innovative Ökosysteme, wie sie z.B. derzeit von mehreren offenen Marktplätzen angeboten werden, müssen mit kontinuierlichen Daten- und Szenario-Pipelines mit mindestens TRL 7 Reifegrad verknüpft werden. Ein konkretes Beispiel wäre die kontinuierliche Aktualisierung von hochauflösenden Karten und deren Ausstattung mit den dringend benötigten Informationen über sensorrelevante Materialdaten (z.B. Reflexions- und Brechungseigenschaften für Radar und Lidar). Solche durchgängigen Integrationsketten sind notwendig, um die erforderliche Qualität der gesamten Datenlieferkette für die Verifikation und Validierung zu erreichen.

Aktualisierte und harmonisierte Szenario-DBs

Szenariobasierte Prüfmethoden, wie sie durch die Projekte der PEGASUS-Familie initiiert wurden, haben die Entwicklung mehrerer Szenario-Datenbankprojekte und sogar erster Szenario-Marktplätze speziell für den Sicherheitsfall angeregt. Diese Szenario-Datenbanken sind zum Teil bereits durch entsprechende Normungsaktivitäten harmonisiert, z.B. Prozessansichten durch ISO und technische Spezifikationen durch ASAM und andere. Mit der Fertigstellung relevanter Normen für szenariobasierte Tests im Jahr 2024 und den bestehenden Vorschriften in Europa aus dem Jahr 2022 könnten neue Bemühungen zur Harmonisierung von Szenario-DBs erforderlich sein, um die geplante Einführung des automatisierten Fahrens zu unterstützen.

Eine solche Datenbank könnte von einem unabhängigen Gremium verwaltet werden und ähnlich wie die deutsche GIDAS-Unfalldatenbank strukturiert sein und sollte logische Szenarien und die erforderlichen Parametertypen sowie Bandbreiten für die Parameter und zusätzliche Metriken enthalten. Eine solche Datenbank muss bestehende Szenario-DBs kombinieren, mit den jüngsten Ergebnissen der oben genannten Initiativen aktualisiert werden und alle relevanten Anforderungen der Interessengruppen aus Industrie, Regulierung und Wissenschaft berücksichtigen.

3.1.2.10.3.2 Risikohandhabung und Anwendung des Sicherheitsnachweises

Anwendung der Risikomodellierung

Im Rahmen von VV-Methoden haben wir einen Prozessrahmen mit dem Ziel der expliziten Darstellung und Verwaltung von Risiken entwickelt - den Risk Management Core. Der konzeptionelle Rahmen basiert auf bestehenden Sicherheitsstandards und wurde auf die spezifische Herausforderung der Verfeinerung einer Verhaltensspezifikation eines automatisierten Fahrsystems angewendet. Während wir diese Anwendung des Risikomanagementkerns in einer Forschungspublikation illustriert haben, gibt es offene Fragen bezüglich weiterer Anwendungen des Rahmens. Insbesondere die Anwendung des Schrittes "Risikomodellierung" innerhalb des Risk Management Core birgt mehrere Herausforderungen. So werden beispielsweise Methoden benötigt, um geschätzte Risiken aus mehreren Szenarien zu einer Schätzung auf ODD-Ebene zu aggregieren. Außerdem müssen Risikoakzeptanzkriterien sowohl auf der ODD-Ebene als auch auf der szenariospezifischen Ebene angewendet werden.

Die Rolle des Risikomanagements für Security / Cybersecurity

Die unterschiedlichen Sicherheitsanforderungen sowie die Auswirkungen der jeweiligen risikomindernden Maßnahmen wirken sich differenziert auf das Risiko des Fahrzeugs aus. Im Risk Management Core, einem wesentlichen Element der VVM-Methode, werden die semantisch abstrahierten Anforderungen zusammengeführt und mit den Anforderungsklassen und deren Labels verglichen. Hier können z.B. Risiken aus der funktionalen Sicherheit und SOTIF kombiniert werden. Daher können Anforderungen der Sicherheit/Cybersecurity mit diesem Ansatz auf die gleiche Weise zusammengeführt und bewertet werden. Wesentlich ist jedoch, dass die Risiken aus Safety und Security in einer gemeinsamen Betrachtung zusammengeführt werden. Dementsprechend müssen auch Zielkonflikte von Safety- und Security-Maßnahmen über weitere Regelwerke (meist unter Einbeziehung eines erweiterten Kontextes) geklärt werden.

Anwendung des Sicherheitsnachweises auf konkrete ODDs

Safety-by-Design auf der Grundlage virtueller Elemente stellt sehr hohe Anforderungen an Modellierungsverfahren, Datenqualität und Rückverfolgbarkeit, systemtechnische Ansätze zur Testorchestrierung und Interoperabilität aller beteiligten Elemente. "Elemente" bedeutet auch

Modellierungsunsicherheiten. Unsicherheiten sollten quantifiziert werden, um den Prozess der V&V sowie die Sicherheit der AD zu verbessern. Der Umgang mit Unsicherheiten ist der Schlüssel zur Industrialisierung von AD und sogar von SAE L2 Funktionen. Systematische nationale und auch multinationale Ansätze, wie szenariobasierte, auf Unsicherheiten basierende Testmethoden in die industrielle Anwendung übertragen werden können, fördern die notwendige Transformation von wissenschaftlichen in industrielle Prozesse. Gleichzeitig bezieht diese Transformation alle und möglicherweise neue relevante Akteure mit ein, die als Bindeglied zwischen bestehenden Testkapazitäten und -einrichtungen dienen können.

3.1.2.10.3.3 3.3 Technologische Herausforderungen

Explizite Spezifikation des Soll-Verhaltens

Die ISO 21448 liefert erste Richtlinien für die Spezifikation des sicheren Sollverhaltens, das ein automatisiertes Fahrsystem in seinem Kontext zeigen soll. Es gibt jedoch keine in der Norm referenzierten Methoden, die in einem industriellen Umfeld angewendet werden können. Daher hat VVMethoden Ansätze zur Erstellung einer Verhaltensspezifikation vorgeschlagen, die zur Unterstützung von Sicherheitsanalysen im Kontext von SOTIF (aber auch im Kontext der funktionalen Sicherheit gemäß ISO 26262) verwendet werden können. Während diese Ansätze in einem begrenzten Umfang von Beispielszenarien angewandt wurden, ist eine weitere Untersuchung erforderlich, wie die vorgeschlagenen Methoden in einem größeren Rahmen funktionieren. Darüber hinaus wurde die Wechselbeziehung zwischen Verhaltensspezifikation und technischem Entwurf konzeptionell betrachtet, da sich die VV-Methoden nicht auf den technischen Entwurf konzentrieren. Zukünftige Arbeiten könnten sich darauf konzentrieren, wie eine Verhaltensspezifikation eine nachvollziehbare Spezifikation von technischen Anforderungen unterstützen kann.

Die Rolle der KI im Sicherheitsnachweis

Wie korrespondieren zukünftige KI-Elemente s.a. Trainingsdaten, virtuell generierte Daten, Modelle und KI-generierte Funktionalitäten sowie KI-basierte Entscheidungsalgorithmen mit dem Gesamtsicherheitsnachweis und wie können sie in den Sicherheitsnachweis integriert werden?

Grundsätzlich wird jedes relevante KI-Systemelement im Sinne einer funktionalen Wirkungskette hinsichtlich seines Einflusses auf die Sicherheit in die VVM-Gesamtmethode einbezogen (analog zu den klassischen Elementen). Innerhalb der Gesamtmethode muss jedes Element, ob klassisches Design oder AI-Design, seinen systemischen Bezug zu Funktion, Risiko, Daten und deren Begründung in einer Argumentation bereitstellen. Der KI-spezifische Umgang ist über die Fokusbereiche der ISO PAS 8800 gut beschrieben:

- KI-Lebenszyklusprozesse wie z.B. der Lebenszyklus neuer Daten
- KI-Sicherheitsanforderungen und KI-Sicherheitsmaßnahmen wie z.B. neue Sicherheitsanalysen und neue Daten- und Modellsicherheitseigenschaften.
- Sichere KI-Entwicklung und -Bewertung wie z.B. neue KI-Sicherheitsanalysen oder Feldbetriebsüberwachung

Die Herausforderung und auch der Schlüssel zur Integration von KI-Elementen in die Safety Case Argumentation liegt in der Vergleichbarkeit ihrer Leistungsmetriken und KI-Sicherheitsmethoden.

Anliegenmanagement

Im VVM wurde der Begriff Anliegenmanagement (bzw. concern management) dem Umgang mit "cross-cutting concerns" zugeordnet, wobei "cross-cutting concern" im Sinne des VVM Aspekte oder Phänomene bezeichnet, die einen relevanten Einfluss auf Ansprüche oder Oberziele, in der Regel auf Sicherheit und Leistung des Systems, haben, deren Auswirkungen oder Ursachen aber nicht beliebig weit voneinander getrennt werden können oder darüber eine erhebliche Unsicherheit besteht. Daher muss das übergreifende Anliegen innerhalb des Rahmens zwischen verschiedenen Bereichen koordiniert werden. Querschnittsbelange können technischer Natur sein, wie z.B. der Einfluss des Verwackelns einer Kamera auf die Erkennungsqualität, z.B. aufgrund von Schlaglöchern (technische Notfälle). Querschnittsthemen können auch auf der Anforderungsebene entstehen, z. B. Konflikte, die sich aus widersprüchlichen Sicherheitsanforderungen ergeben.

Das VVM-Konzept des Concernmanagements ist eine Zuordnung von bereichsübergreifenden Belangen zu einer proprietären, domänenübergreifenden Struktur (z.B. Datenstrukturen), die bekannte Einflüsse von bereichsübergreifenden Belangen mit den verschiedenen Domänen verknüpft, wie z.B. den Einfluss von Solar-Glare (Aspekt der ODD-Domäne) auf das Testen von optischen Sensoren (Aspekt der V&V-Domäne). Concern-Management ergänzt somit die Schnittstellen zwischen Meta-Layern, Domänen und deren Hierarchien mit einem Speicher von domänenübergreifenden Entwicklungsherausforderungen oder Problemräumen. Ziel dieser Strukturen ist nicht die Schaffung von Parallelität, sondern die Speicherung von Wissen und die spätere Analyse und Entwicklung der bereichsübergreifenden Belange in dem Maße, dass ihre Einflüsse auf Maßnahmen in den Domänen und deren Schnittstellen übertragen werden können, bis die von ihnen ausgehenden Risiken ausreichend begrenzt sind. Bedenken werden auch durch die Argumentationsstruktur angesprochen. Die Anliegen der Argumentation umfassen die Auswirkungen der Querschnittsanliegen und auch allgemeine Anliegen der Argumentation.

Ferngesteuerter Betrieb

Ferngesteuerter Betrieb als Brückentechnologie zwischen menschengesteuerten Fahrzeugen und Vollautomatisierung könnte eigene Validierungs- und Verifizierungsherausforderungen mit sich bringen, die folglich durch szenariobasierte Testmethoden bewältigt werden müssen. Im Gegensatz zur VVM muss die Beteiligung eines menschlichen Fahrers und insbesondere die Konnektivität zwischen Fahrzeug und Teleoperationsinfrastruktur berücksichtigt werden. Im Falle eines Verlusts oder einer starken Beeinträchtigung der Konnektivität müsste ein Manöver mit minimalem Risiko autonom über bordeigene Systeme ausgeführt werden. Darüber hinaus müssen die maximalen Fahrzeiten eines ferngesteuerten Bedieners und die Auswirkungen auf seine Fähigkeiten sowie die Auswirkungen der Latenzzeiten zwischen Fahrzeug und Teleoperationszentrum (einschließlich der menschlichen Reaktionszeiten) bewertet werden. Viele der in VVM vorgeschlagenen Werkzeuge könnten für diese Analyse verwendet werden, wie das ODD-Metamodell, die Ontologieansätze, Datenformate, Szenario-Datenbanken und die vorgeschlagenen Testmethoden wie Adaptive Replay-to-Sim und Vehicle/Prototype-in-the-Loop.

Kollektives Lernen und Anpassungskonzepte aus dem Praxisbetrieb

Derzeit wird die Erprobung bzw. der Betrieb von automatisierten Fahrsystemen im Feld in verschiedenen Ländern beschleunigt und durchgeführt. Ein systematischer Austausch von nicht-proprietären Daten und Erkenntnissen, die bei diesen Aktivitäten gewonnen werden, kann den Aufwand aller Beteiligten drastisch reduzieren und so als Katalysator für Verbesserungen wirken. Im Idealfall führt dies zu mehr Sicherheit, noch bevor die Systeme in den Feldversuch gehen, da

die Beteiligten die Möglichkeit haben, auf sicherheitsrelevante Faktoren und die ihnen zugrundeliegenden Kausalitäten für ihre Ziel-ODD zuzugreifen. Wie kann man aus Felddaten kollektiv lernen? Hier sind eine offene und systemunabhängige Wissensbasis und die entsprechenden Spezifikationen in Übereinstimmung mit den neuesten Standardisierungsparametern und -metriken ein wertvolles Instrument. Ein länderübergreifender System-Engineering-Ansatz, der relevante Daten und Erfahrungen sammelt, auswertet und in den Safety Case sowie in die produktentwicklungsgetriebenen Wertschöpfungsketten einfließen lässt, ist ein vielversprechender Ansatz, um die Sicherheit zu erhöhen und den Aufwand zu reduzieren.

3.2 Nutzen und Verwertbarkeit

VVM als vorwettbewerbliches Verbundprojekt hatte das definierte Ziel die Entwicklung von autonomen Fahrfunktionen durch die in Kapitel 2.1"Aufgabenstellung" beschriebenen Ergebnisse voranzubringen. Die konkreten Verwertungspläne der einzelnen Partner sind naturgemäß in den partnerspezifischen Abschlussberichten zu finden. Es ergibt sich aber zusätzlich eine projektweite Perspektive, denn das Forschungsfeld unterlag und unterliegt nicht nur einer großen Dynamik, sondern es stößt in seinem grundsätzlichen Bestreben völlig neue Türen auf. Die zu lösenden Fragen gehen in Komplexität und Tiefe deutlich über das Maß hinaus, welches in früheren Jahrzehnten für die Weiterentwicklung im Automobilbau üblich war. Das betrifft auch nachgelagerte Schritte der Ordnungs- und Zulassungsbehörden. Insofern war es unbedingt nötig, dass VVMethoden mit der Fachcommunity und speziell Stakeholdern außerhalb des Projektes in einen fruchtbaren Austausch tritt, um gemeinsam und mit den übergeordneten Gremien und Institutionen Konzepte und Lösungen zu diskutieren.

Unter anderem aus diesem Grund wurden im Lauf der Projektanbahnung entsprechende Aktivitäten vorgesehen und in einem zusätzlichen TPX verortet. TPX hat während der Projektlaufzeit kontinuierlich Kontakt zu externen Stakeholdern gehalten und Zwischenergebnisse beziehungsweise finale Resultate eingebracht. In VVMethoden selbst wurden die dazu nötigen Abstimmungen durchgeführt um mit konsolidierten Positionen wertvolle Beiträge leisten zu können. Es wurden Materialien auf qualitativ hohem Niveau erstellt, die dann von den jeweiligen Fachexperten aus dem Projekt und der Projektkoordination vorgestellt und diskutiert wurden.

Als weitergehende Maßnahme zur Vertiefung des Austauschs wurde auch entschieden regelmäßig entsprechende Dokumente aus dem Projekt freizugeben, es wurde auch ein dezidierter Steuerkreisbeschluss gefasst um deren Freigabe zu vereinfachen. Die Veröffentlichung unter anderem der finalen Deliverables und der Prozessschaubilder auf der öffentlichen Webseite des Projektes stellen einen weiteren Weg dar, um sicherzustellen, dass die Projektergebnisse auch Stakeholdern außerhalb des Projektes zugänglich sind und in der Fachwelt diskutiert und weiterentwickelt werden können.

Die Austauschaktivitäten sind in Kapitel 3.1.2.10 TPX näher beschrieben, sie betrafen sowohl andere Projekte und Initiativen sowie Gremien und Institutionen wie zum Beispiel:

- ADscene
- HEADSTART
- SAKURA
- Die Projekte der VDA Leitinitiative autonomes und vernetztes Fahren

- ISO WG 13
- Bundesministerium für Digitales und Verkehr (BMVI)

3.3 Projekt Impact

Der fachliche Impact des Projektes VVMethoden besteht vor allem in dem Zurverfügungsstellen einer industriell verwertbaren Gesamtmethodik zum Nachweis der Sicherheit einer automatischen Fahrfunktion sowie derer Subkomponenten. Dazu werden im Wesentlichen 4 zur industriellen Nutzung geeignete Perspektiven auf die Gesamtmethode zur Verfügung gestellt. Diese sind auch in einer verfügbar, so dass sich die Ergebnisse ideal an bisherige firmeninterne Abläufe anpassen lässt.

Das VVM-Projekt bietet einen Rahmen als Grundlage für eine systematisch begründete und methodisch gestützte Zulassung von Automatischen Fahrfunktionen (ADS) mit Schwerpunkt auf der industriellen Umsetzung. Es baut auf dem PEGASUS-Ansatz mit der Weinführung szenarienbasierter Testmethodiken auf und geht auf die besonderen Herausforderungen von ADS in der Komplexität des Stadtverkehrs und offener Kontexte ein. Die VVM-Methodik bewältigt die hohe Komplexität des Verkehrs und des offenen Kontextes unter anderem durch fünf sich gegenseitig ergänzende Handlungsstränge die durch das Projekt entwickelt und differenziert ausgearbeitet wurden.

Safety-by-Design - VVM integriert die ADS-Sicherheit systematisch in den Entwicklungs- und Konstruktionsprozess vom ersten Schritt an und sorgt für die digitale Rückverfolgbarkeit der zugehörigen Arbeitsprodukte bis hin zur Verifikation und Validierung.

Erklärbarkeiten für gesellschaftliche Sicherheitserwartungen - Entwicklung einer systematischen Argumentation zur Begründung der Erfüllung der Sicherheitserwartungen der Gesellschaft an die ADS-Technologie. Die Sicherheitsargumentation wird durch eine strukturierte Zerlegung der Top-Level-Sicherheitsaussage "Abwesenheit von unzumutbarem Risiko" in realisierbare Teilaussagen für den ADS-Betrieb erreicht, wobei eine konsistente Verwendung von Metriken gestärkt wird.

Ende-zu-Ende-Risikomanagement - Zerlegung von Sicherheits-Teilaussagen für das Verhalten des Gesamtsystems in Risikoaspekte, Einsatz von Risikomaßnahmen im Systementwurf und Verknüpfung von Risikoaspekten mit szenarienbasierten Nachweisen in der V&V, wodurch eine Gesamtkontrolle der Risikoakzeptanz ermöglicht wird.

Verbesserte Virtualisierung der Absicherung - Effizienz durch Verlagerung so vieler Tests wie möglich in die Simulation bei gleichzeitiger Sicherstellung von evidenzbasierten Testergebnissen durch nahtlose Integration von Prüfstandstests und realen Flottendaten sowie die konsistente Verwendung von Metriken.

Erweiterterung des szenarienbasierten Ansatzes als Metamodell für die Produktbeschreibung in Form der ODD, der eine zielgerichtete Zerlegung der ODD entsprechend dem Design eines ADS ermöglicht und als Referenzmodell für die Argumentation der ADS-Leistung im Verifikations- und Validierungsprozess dient.

Die VVM Gesamtmethode

Die Entwicklung eines ADS ist eine komplexe Aufgabe, an der viele Interessengruppen aus verschiedenen Bereichen und meist auch verschiedene Unternehmen entlang der automobilen

Wertschöpfungskette beteiligt sind. VVM hat eine Methodik entwickelt die künftig als gemeinsame Grundlage für die Entwicklung und Absicherung zukünftiger automatisierter Fahrsysteme (ADS) mit einem gesellschaftlich akzeptierten Risiko vorgeschlagen wird. Das VVM-Rahmenwerk integriert alle Perspektiven die für die Entwicklung eines sicheren ADS erforderlich sind, indem es Simulationsstrategien mit Prüfständen und Straßentests verbindet und so eine praktikable Validierung und Verifizierung (V&V) ermöglicht. Umfassend, strukturiert sowie integrierbar in etablierte industrielle Prozesse.

PEGASUS, das Vorgängerprojekt von VVM, konzentrierte sich auf das Testen. Es etablierte szenarienbasierte Tests in vernetzter Simulation in Kombination mit Prüfstandsversuchen und realen Fahrten, um eine positive Bilanz bzw. ein reduziertes Unfallrisiko eines ADS in seiner ODD nachzuweisen. PEGASUS führte auch eine Szenario-Datenbank als Informationsgrundlage ein. VVM erweitert diesen Ansatz einschließlich des Entwicklungsprozesses mit seinen Abhängigkeiten von aktuellen Normen (z.B. FUSA und SOTIF) zu einer umfassenden Sicht auf die Sicherheit von ADS. Im Kern strukturiert VVM die komplexen Anforderungen des betrieblichen Konstruktionsbereichs in einem Detaillierungsgrad, der es ermöglicht, eine Funktion so zu entwickeln, dass sie in diesem Bereich sicher betrieben werden kann. Darüber hinaus ermöglicht VVM eine Argumentation der Sicherheit gegenüber der Gesellschaft. VVM hat einen prozessualen Rahmen vorgeschlagen der aus vier unterschiedlichen Perspektiven besteht:

- **Die globale Entwicklungs- und V&V-Perspektive**, die sich auf die Vorbereitung des produktentwicklungsnahen V-Modells für die Integration der Argumentation konzentriert und die Beweisführung aus dem Design- und V&V-Prozess innerhalb der Argumentation sicherzustellen

- **Die szenarienbasierte Entwicklungs- und Testperspektive** konzentriert sich auf den Prozess von der Produktentwicklung, insbesondere dem sicheren Verhalten, bis zur V&V Architektur. Sie erweitert den etablierten Produktentwicklungsprozess um einen Ansatz zur konsistenten Verwendung ein- und desselben Szenario-Metamodells während des gesamten Entwicklungs- und Nachweisprozesses.

- **Die Risikomanagement-Perspektive** konzentriert sich auf ein integriertes Konzept zur Behandlung von Risiko und dessen Integration in Sicherheitsnachweis gemäß der vorstehend genannten Perspektiven.

- **Die Sicherheitsargumentationsperspektive** führt eine Sicherheitsargumentation mit dem Ziel, Sicherheit eines ADS über Argumentationen und Sub-Beweise zu führen

Im Folgenden werden diese vier Perspektiven vertiefend erläutert. Zu jedem dieser 4 Perspektiven sind in den Projektergebnissen neben detaillierten Veröffentlichungen auch industriell anwendbare Prozessübersichten und Flowcharts erhältlich.

Perspektive Globale Entwicklung und V&V

Die globale Entwicklungs- und V&V-Perspektive konzentriert sich auf die konzeptionellen Blöcke, die im Entwicklungsprozess eines ADS vorhanden sind, und verbindet diese mit den drei Ebenen, entsprechend den Ansichten für die Sicherheitsargumentation

- **Die Fähigkeitsschicht** konzentriert sich auf die Zusammenstellung abstrakter Anforderungen. Relevante Forderungen, z. B. gesellschaftliche, gesetzliche, normative

oder die beabsichtigten Funktionen werden in ADS-Verhaltensweisen entsprechend ihrer ODD und in zugehörige Fähigkeiten, einschließlich der für V&V erforderlichen Fähigkeiten, übertragen.

- **Der Engineering Layer** konzentriert sich auf die Test-Systemspezifikation, strukturiert die Zerlegung der abstrakten Anforderungen in die Entwurfsspezifikationen der ADS sowie der Tests zur Validierung und Verifizierung.
- **Der Real World Layer** konzentriert sich auf die Interaktion der endgültigen Implementierung mit der realen Welt und ermöglicht so die Validierung des ADS-Verhaltens in einer unkontrollierten Umgebung.

Dieser umfassende Ansatz bietet eine effiziente und nachvollziehbare Dekomposition von Design und V&V. Die Dekomposition wird durch das Risikomodell und das ODD-Metamodell angeführt. Auf diese Weise werden Design und V&V so strukturiert, dass die Argumentation der Systemsicherheit durch eine zielgerichtete Argumentation unterstützt wird.

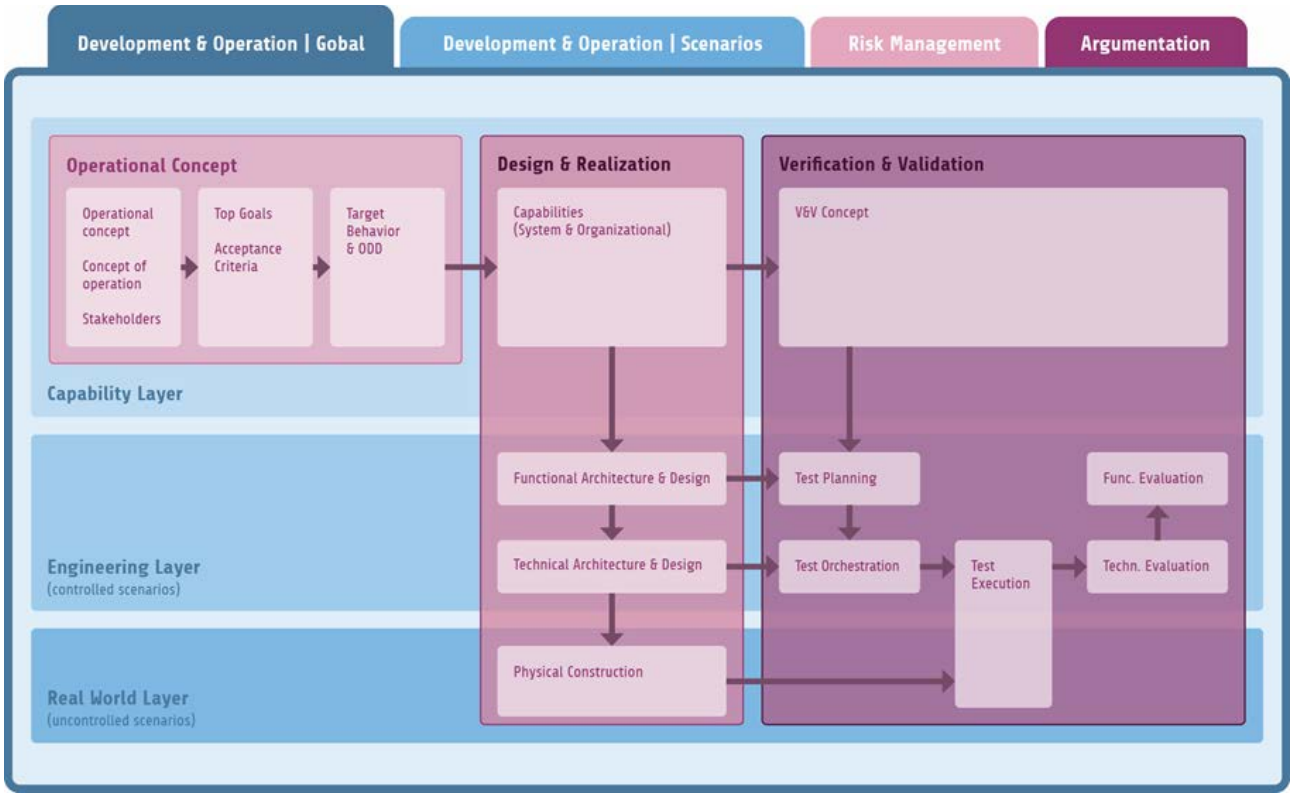


Abbildung 290: Globale Entwicklung und V&V-Methode

Perspektive szenarienbasierte Entwicklung und Prüfung

Ergänzend zur konzeptionellen Sichtweise konzentriert sich die Perspektive der szenarienbasierten Entwicklung und Prüfung auf den Ansatz, wie szenarienbasierte Methoden zur Ergänzung des Entwicklungs-, Bestätigungs- und Gewährleistungsprozesses eines sicheren ADS eingesetzt werden können. VVM schlägt vor, den Entwicklungsprozess auf einen frühen Abgleich von Artefakten und Sicherheitsanforderungen, die aus Sicherheitsargumenten abgeleitet werden, sowie auf einen Abgleich der Formulierung der Anforderungen, die später im Validierungs- und Verifizierungsprozess als Nachweis verwendet werden, zu erweitern.

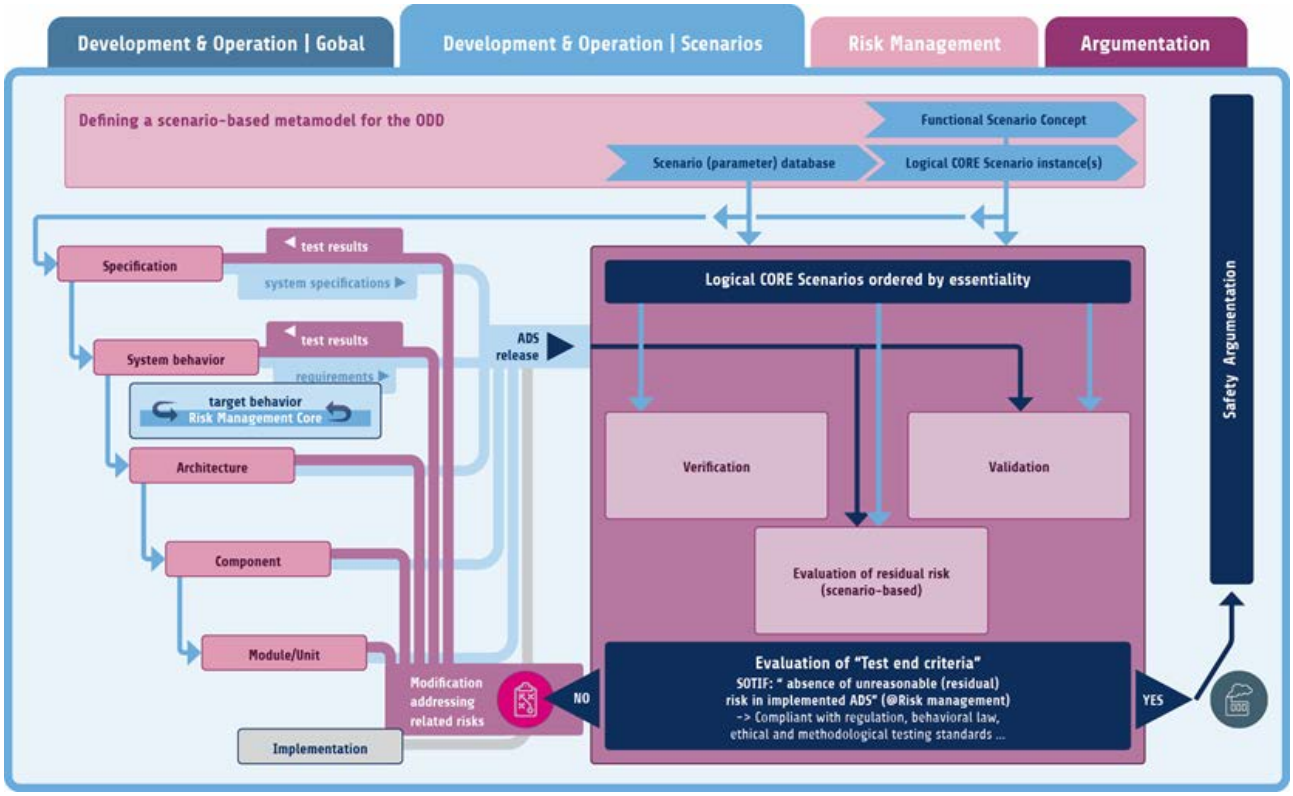


Abbildung 291: Szenariobasierte Entwicklung und Prüfung

Mit Blick auf die Sicherheitsargumentation wird das ODD-Metamodell, das aus einer Reihe von Kernszenarien besteht, als ein neues Werkzeug eingeführt, das sowohl im Entwurfs- als auch im V&V-Prozess eingesetzt werden kann. Die Einführung des ODD-Metamodells im Entwurfsprozess ermöglicht es, die Problemraumanalyse, den Systementwurf und die Absicherung des Systems auf der gleichen Menge von Szenarien durchzuführen, die die ODD darstellen. Die Problemraumanalyse liefert ein tiefes Verständnis des Problemraums: Sie kann als Grundlage für das SOTIF dienen.

Gefahren- und Risikoanalyse, die Definition von Sicherheitszielen sowie die Integration der Bedürfnisse von Interessengruppen (z. B. rechtlicher, gesellschaftlicher oder ethischer Art) in das Systemverhalten und den Entwurf. Darüber hinaus dient das Kernstück des Risikomanagements, das einen Prozessrahmen für das Risikomanagement insbesondere im Zusammenhang mit der Spezifikation des Systemverhaltens und dem Umgang mit gefährlichen Ereignissen definiert, der konsequenten Nutzung kontrollierter und verwalteter Risiken während der gesamten Entwicklung und Absicherung.

Während der Validierung und Verifizierung: Die Verwendung des ODD-Metamodells ermöglicht die V&V auf demselben ODD-Metamodell wie die Gefahren- und Risikoanalyse und das Systemdesign. Daraus ergibt sich die neue V&V-Aufgabe der Validierung der ausreichenden Gültigkeit des aktuellen Satzes von CORE-Szenarien. In dieser Aufgabe muss der Nachweis erbracht werden, dass das CORE-Szenario und die zugehörigen Eigenschaften die realen Szenarien der Zieldomäne angemessen abdecken. Hinzu kommt die Bewertung der Maßnahmen, die sich aus dem risikobeherrschten Systemverhalten ergeben, wobei nachzuweisen ist, dass sich das System zumindest so verhält, dass die Risikoakzeptanzkriterien in seiner ODD erfüllt sind. Und das V&V-Konzept erhält einen Fokus auf eine versicherungsbezogene Organisation der V&V: Testobjekte, Testziele, Testebenen, Testplattformen und Teststrategien werden durch das V&V-

Konzept miteinander verknüpft und auf den Bedarf an Artefakten und Nachweisen für den Aufbau des Sicherheitsarguments abgestimmt.

Mit der Einführung des Metamodells ODD werden die Anforderungen an das System vorstrukturiert, was eine intelligente Integration von Simulationsstrategien, Prüfständen und Praxistests sowie eine ganzheitliche, praktikable Validierung ermöglicht, die schon früh in der Entwicklung beginnt und ein integraler Bestandteil des Entwicklungsprozesses ist.

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.

Die Risikomanagement-Perspektive

Die Risikomanagementperspektive wird als Teil des VVM-Rahmens eingeführt, da sie als Grundlage für mehrere Zwecke dienen kann. Die Risikomanagement-Perspektive sammelt alle Gefahren und Sicherheitsziele des ADS und ermöglicht die Definition eines sicheren Zielverhaltens, den Abgleich von Systemrisiken mit Akzeptanzkriterien, die Risikoabschätzung spezifischer Systemelemente sowie die Risikobewertung zu Beginn des Produktionszyklus des ADS.

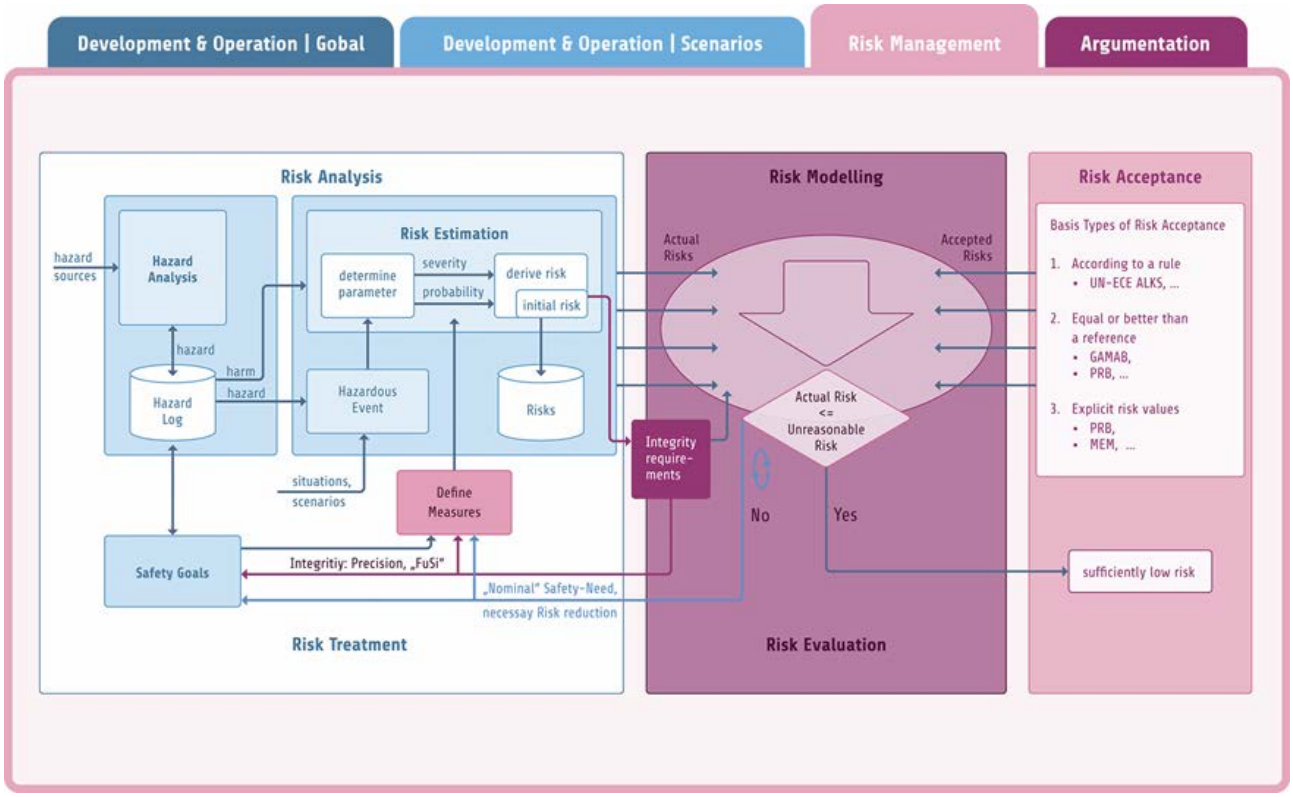


Abbildung 292: Risikomanagement

Die Vielzahl der notwendigen Sicherheitsbetrachtungen, sei es die Sicherheit der beabsichtigten Funktion, die funktionale Sicherheit und andere, müssen verwaltet werden. Zu diesem Zweck wird innerhalb des VVM-Rahmens die Perspektive des Risk Management Core (RMC) eingeführt. Der RMC steht für die kontinuierliche Bearbeitung tatsächlicher Risiken, um sie mit akzeptablen

Risiken in Einklang zu bringen. Er legt das Risiko als führendes Maß für die Sicherheit fest, fasst alle Systemrisikoaspekte zusammen und gleicht das Systemrisiko mit Risikoakzeptanzkriterien ab

Die Sicherheitsargumentationsperspektive

Die Perspektive der Sicherheitsargumentation wird innerhalb des VVM-Rahmens eingeführt, um zu begründen, warum ein ADS sicher ist, d.h. warum während des Betriebs keine unzumutbaren Risiken bestehen. Diese Perspektive wird vorgeschlagen, um alle Quellen von ADS-Risiken zu erfassen und die Art und Weise zu strukturieren, wie die oberste Sicherheitsbehauptung "Abwesenheit von unzumutbaren Risiken" in handhabbare Unterbehauptungen zerlegt wird. Beweise aus allen Perspektiven des VVM-Zuverlässigkeitsrahmens werden im Sicherheitsargumentationsprozess verwendet.

Der Risikomanagement-Kern wird als Referenzmodell verwendet, um die Übereinstimmung des geschätzten Risikos mit dem akzeptierten Risiko zu begründen. Der szenarienbasierte Entwicklungs- und Testansatz dient als Referenzmodell, um zu begründen, dass die ADS-Entwicklung und -V&V Vertrauen schafft. Die globale Entwicklung und V&V dient als Grundlage dafür, dass die Spezifikation der erforderlichen Fähigkeiten, ihre Entwicklung und Validierung unter kontrollierten und unkontrollierten realen Bedingungen abgeschlossen sind.

Die VVM-Sicherheitsargumentationsperspektive strukturiert den Argumentationsbedarf für die ADS-Risikovorhersage auf der Grundlage von Annahmen über relevante Entwicklungs- und V&V-Artefakte. Sie dient als Ausgangspunkt für die Argumentationsentwicklung in konkreten ADS-Projekten unter Berücksichtigung unternehmensspezifischer Sicherheitsmethoden und V&V.

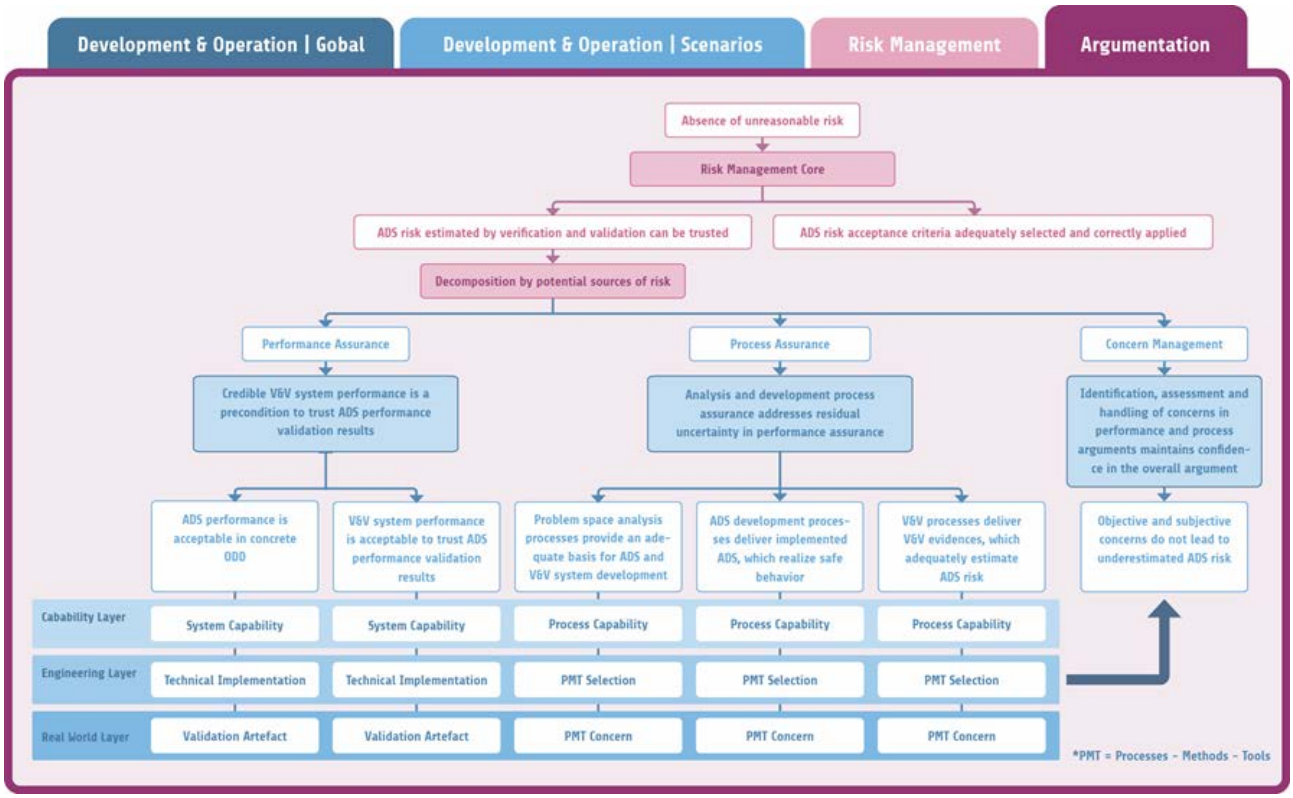


Abbildung 293: Sicherheitsargumentation

Schlussfolgerung

Alle vier Perspektiven des VVM-Gesamtrahmens vereinen die wichtigsten Aspekte, um sicherzustellen, dass von einem ADS kein unangemessenes Risiko ausgeht. Somit trägt VVM dazu bei, die Transparenz und Akzeptanz des Sicherheitsgewährleistungsprozesses durch diese umfassende Methode zu erhöhen. Die Anwendung

einer Sicherheitsargumentation erfordert eine konsequente Ausrichtung der szenarienbasierten Entwicklung und Prüfung, umfassendes Risikomanagement und Argumentation sowie eine explizite Definition der verbindenden Schnittstellen, um den Open-World-Kontext testfähig zu machen. Dieser Ansatz stärkt unmittelbar die Wettbewerbsfähigkeit, da Unternehmen durch die systematische Integration von Sicherheit in den Entwicklungs- und Testprozess einen entscheidenden Vorteil erlangen können.

4 Veröffentlichungen

- Lukas Westhofen, Christian Neurohr: Answering Temporal Conjunctive Queries over Description Logic Ontologies for Situation Recognition in Complex Operational Domains. : In TACAS '24, Luxembourg, Luxembourg, 04.2024
- Christian Neurohr, Lukas Westhofen, Tuan Duong Quang, Tjark Koopmann, Roman Gansch, Stefan Schnoenawa: Requirements on Simulation Systems and Models Posed by a Criticality Analysis for Automated Driving Systems.
- Christian Neurohr, Lukas Westhofen, Martin Butz, Martin Bollmann, Lina Putze, Tjark Koopmann, Roman Gansch, Michael Knoop, Armin Rasch, Bogdan Cojocaru, Johannes Daube: Advances on the Criticality Analysis for Automated Driving Systems.
- Nayel Fabian Salem Christian Lalitsch-Schneider Marcus Nolte Jan Reich Dr. Tino Brade Marco Fistler: Transition from a Top-Level to a Low-Level Argumentation.
- Max Nestoriuc, Himanshu Walia: Criticality driven data acquisition in autonomous driving. : In ELIV Europe 21st International Congress and Exhibition, Bonn, 18-19.10.2023
- Lukas Westhofen: Answering Temporal Conjunctive Queries. In Vancouver, Canada, 02.2024
- Bangarevva Patil, Thomas Corell, Rudra Narayan Hota: In-Service Monitoring and Assessment of AD vehicles with AI based Algorithms. In: Valencia, Spain, 13-17.11.2023
- Helen Gremmelmaier, Lukas Hierzegger, Mohammed Sohail M, und J. Marius Zöllner: Cyclist's behavior: a survey on characteristics and trajectory modeling. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24-28.09.2023
- Barbara Schütt Meng Zhang, Christian Steinhauser Eric Sax: Evolutionary Behavior Tree Generation for Dynamic Scenario Creation in Testing of Automated Driving Systems. In: The 7th International Conference on System Reliability and Safety Bologna, Italy, 22.-244.11.2023
- Henning Mosebach, Roland Galbas, Jan Reich: The VV Methods safety assurance framework – Final event announcement. In: San Francisco, 12.07.2023
- Himanshu Walia, Max Nestoriuc: VVM Introduction & Criticality based data capturing. In: Innovation Park Allgaeu Airport, Germany, 22.06.2023
- Max Zipfl, Sven Spickermann, J. Marius Zöllner: Utilizing Hybrid Trajectory Prediction Models to Recognize Highly Interactive Traffic Scenarios. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023
- Marc René Zofka, Tobias Fleck, Philip Schörner, Marc Heinrich, J. Marius Zöllner: Paving the Ways for Vehicles-in-the-loop: Wireless Integration of Autonomous Vehicles into Mixed Reality Proving Grounds and Test Areas. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023
- Patrick Schulz, Alexander Viehl, Oliver Bringmann: Towards Fast Environment Generation Methods for Virtual Testing. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023
- Christoph Glasmacher, Lutz Eckstein: Acquire Driving Scenarios Efficiently: A Framework for Prospective Assessment of Cost-Optiaml Scenario Acquisition. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023

- Kai Storms, Ken Mori, Steven Peters: Defining and Validating Urban Object Relevance for Collision Safety. In: 15. Uni-DAS e.V. Workshop Fahrerassistenz und automatisiertes Fahren, Berkheim, 24.10.2023
- Max Zipfl, Moritz Jarosch, J. Marius Zöllner: Traffic Scene Similarity: a Graph-based Contrastive Learning Approach. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023
- Nayel Fabian Salem, Veronica Haber, Matthias Rauschenbach, Marcus Nolte, Robert Graubohm, Jan Reich, Torben Stolte, Markus Maurer: Semantische Normverhaltensanalyse zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge. In: 15. Uni-DAS e.V. Workshop Fahrerassistenz und automatisiertes Fahren, Berkheim, 24.10.2023
- Barbara Schütt ,Stefan Otten , Eric Sax: Exploring the Range of Possible Outcomes by means of Logical Scenario Analysis and Reduction for Testing Automated Driving Systems. In: ITSC 2023 Bilbao, Bizkaia, Spain, 24.-28.09.2023
- Martin Bollmann, Armin Rasch: Diskussion von Kritikalitätsphänomenen. In: WOST Conference, Ettersburg Castle, Weimar, 22.06.2023
- Lukas Elster, Philipp Rosenberger, Martin Holder, Ken Mori, Jan Staab, Steven Peters: Introducing the Double Validation Metric for Radar Sensor Models. In: AAET Journal
- Roland Galbas: Result from German project “VV-Methods” – VVM building blocks for safety assurance. In: ITS Lisbon, 24.05.2023
- Ferdinand Mütsch, Helen Gremmelmaier , Nicolas Becker, Daniel Bogdoll, Marc René Zofka, J. Marius Zöllner: From Model-Based to Data-Driven Simulation: Challenges and Trends in Autonomous Driving. In: CVPR, Vancouver, CA, 18.-22.06.2023
- Thomas Kirschbaum Dr. Tino Brade Nayel Fabian Salem Marcus Nolte Christian Lalitsch-Schneider Jan Reich: Erfüllung gesellschaftlicher Sicherheitserwartungen. Explizite Risikobetrachtung und Sicherheitsargumentation für hochautomatisierte Fahrzeuge. In: safe.tech 2023, München, 23.5.2023
- Thomas Kirschbaum, Nayel Fabian Salem, Marcus Nolte, Christian Lalitsch-Schneider Robert Graubohm, Roland Galbas: The “Risk Management Core”. TRB: Automated Road Transportation Symposium, San Francisco, USA, 12.07.23
- Nayel Fabian Salem Thomas Kirschbaum Marcus Nolte Christian Lalitsch-Schneider, Robert Graubohm, Markus Maurer: Risk Management Core – Towards an Explicit Representation of Risk in Automated Driving. In: Safety Week Autonomobil, Würzburg, 23.05.23
- Hendrik Weber, Christoph Glasmacher, Michael Schuldes, Nicoals Wagener, Lutz Eckstein: Holistic Driving Scenario Concept for Urban Traffic. In: IEEE IV 2023, Anchorage, Alaska, USA, 04.06.23
- Nayel Fabian Salem, Thomas Kirschbaum, Marcus Nolte, Christian Lalitsch-Schneider, Robert Graubohm, Jan Reich, Markus Maurer: Risk Management Core – Towards an Explicit Representation of Risk in Automated Driving. In: IEEE Access, 2023

- Barbara Schütt, Maximilian Zipfl, J. Marius Zöllner, Eric Sax: Inverse Universal Traffic Quality - a Criticality Metric for Crowded Urban Traffic Scenes. In: IEEE IV 2023, Anchorage, Alaska, USA, 04.06.23
- Max Zipfl, Nina Koch, and J. Marius Zöllner: A Comprehensive Review on Ontologies for Scenario-based Testing in the Context of Autonomous Driving. In: IEEE IV 2023, Anchorage, Alaska, USA, 04.06.23
- Barbara Schütt, Joshua Ransiek, Thilo Braun, Eric Sax: 1001 Ways of Scenario Generation for Testing of Self-driving Cars: A Survey. In: IEEE IV 2023, Anchorage, Alaska, USA, 04.06.23
- Lina Putze, Lukas Westhofen, Tjark Koopmann, Eckard Böde, Christian Neurohr: On Quantification for SOTIF Validation of Automated Driving Systems. In: IEEE IV 2023, Anchorage, Alaska, USA, 04.06.23
- Julian Fuchs, Thilo Braun, Lennart Ries, Eric Sax: Similarity analysis of concrete scenarios in the context of virtual scenario-based validation of vehicles. In: IEEE Intelligent vehicles symposium, Alaska, 04.06.23
- Kai Storms, Ken Mori, Steven Peters: Conservative Estimation of Perception Relevance of Dynamic Objects for Safe Trajectories in Automotive Scenarios. In: IEEE International Conference on Mobility, Detroit, Michigan, USA, 17.05.2023
- Christoph Glasmacher, Hendrik Weber, Michael Schuldes, Nicolas Wagener, Lutz Eckstein: Generation of Concrete Parameters from Logical Urban Driving Scenarios based on Hybrid Graphs. In: VEHITS, Prag, 26.04.2023
- Henning Mosebach, Marcus Nolte, Jan Reich, Roland Galbas: From safety argumentation to an assurance framework - The PEGASUS projects SET Level and VV Methods. In: SIP-adus Workshop 2022, Kyoto, Japan, 12.10.2022
- Jan Reich: The safety assurance architecture of VV Methods. In: SIP-adus Workshop 2022, Kyoto, Japan, 13.10.2022
- Katrin Lotto, Thomas Nagler, Mladjan Radic: Modeling Stochastic Data Using Copulas For Application in Validation of Autonomous Driving. In: Electronics - MDPI, 13.12.2022
- Roland Galbas, Christian Neurohr, Philipp Rosenberger, Gerhard Schunk: Application of SET Level results in the VVMethods Project. In: SetLevel Abschlussveranstaltung, 11./12.10.2022
- Tjark Koopmann, Christian Neurohr, Lina Putze, Lukas Westhofen, Roman Gansch, Ahmad Adee: Grasping Causality for the Explanation of Criticality for Automated Driving. In: ACM Transactions on Intelligent Systems and Technology (TIST), 27.10.2022
- Tobias Merk, Dr. Andreas Linnemann, Martin Herbert Bollmann, Dr. Mladjan Radic: MerLin potential based ciriticality measure. In: In: Organisation durch Cornell University, 17.08.2022.
- Nayel Fabian Salem, Veronica Haber, Matthias Rauschenbach, Marcus Nolte, Jan Reich, Robert Graubohm, Torben Stolte, Markus Maurer: Ein Beitrag zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge. 15.09.2022

- Clemens Linnhoff, Kristof Hofrichter, Lukas Elster, Philipp Rosenberger, Hermann Winner: Measuring the Influence of Environmental Conditions on Automotive Lidar Sensors. In: MDPI Sensors, 07/2022.
- Lukas Westhofen, Christian Neurohr, Tjark Koopmann, Martin Butz, Fabian Utesch, Christian Gutenkunst, Eckard Böde: Criticality Metrics for Automated Driving: A Review and Suitability Analysis of the State of the Art. In:Archives of Computational Methods in Engineering.
- Lukas Westhofen, Christian Neurohr, Martin Butz, Maike Scholtes, Michael Schuldes: Using Ontologies for the Formalization and Recognition of Criticality for Automated Driving. In: IEEE Open Journal of Intelligent Transportation Systems.
- Clemens Linnhoff, Philipp Rosenberger, Hermann Winner: Refining Object-Based Lidar Sensor Modeling — Challenging Ray Tracing as the Magic Bullet. In: IEEE Sensors Journal, 01.11.2021.
- Cheng Wang, Kai Storms, Hermann Winner: Online Safety Assessment of Automated Vehicles Using Silent Testing. In: IEEE Transaction on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3119546.
- Clemens Linnhoff, Philipp Rosenberger, Simon Schmidt, Lukas Elster, Rainer Stark, Hermann Winner: Towards Serious Perception Sensor Simulation for Safety Validation of Automated Driving - A Collaborative Method to Specify Sensor Models. In: IEEE ITSC 2021, Indianapolis, 19.-21.09.2021.
- Stefanie Walz, Mario Bijelic, Florian Kraus, Werner Ritter, Martin Simon, Igor Doric: A Benchmark for Spray from Nearby Cutting Vehicles. In: IEEE ITSC 2021, Indianapolis, 19.-21.09.2021.
- Patrik Schneider, Martin Butz, Christian Heinzemann, Jens Oehlerking, Matthias Woehrle: Towards threat metric evaluation in complex urban scenarios. In: IEEE ITSC 2021, Indianapolis, 19.-21.09.2021.
- Hans Nikolaus Beck, Nayel Fabian Salem, Veronica Haber, Matthias Rauschenbach, Jan Reich: Phänomen-Signal-Modell: Formalismus, Graph und Anwendung. 31.07.2021.
- Maike Scholtes, Lutz Eckstein: Systematic Categorization of Influencing Factors on Radar-Based Perception to Facilitate Complex Real-World Data Evaluation. In: IEEE Intelligent Vehicles Symposium, Nagoya, 11.15.06.2021.
- Matthias Rauschenbach, Christian Wolschke, Tobias Braun, Simon Kupjetz: Ansatz zur methodischen Analyse und Absicherung des Funktionalkonzepts voll automatisierter Kraftfahrzeuge. In: 30. VDI-Fachtagung Technische Zuverlässigkeit 2021, Nürtingen, 27.-28.04.2021.
- Michael Hoß, Maike Scholtes, Lutz Eckstein: A Review of Testing Object-Based Environment Perception for Safe Automated Driving. 2021.
- Lukas Elster, Clemens Linnhoff, Philipp Rosenberger, Simon Schmidt, Rainer Stark, Hermann Winner: Fundamental Design Criteria for Logical Scenarios in Simulation-based Safety

Validation of Automated Driving Using Sensor Model Knowledge. In: 32nd International Vehicle Symposium.

- Clemens Linnhoff, Philipp Rosenberger, Martin Friedrich Holder, Nicodemo Cianciaruso, Hermann Winner: Highly Parameterizable and Generic Perception Sensor Model Architecture. In: 6. Internationale ATZ-Fachtagung Automatisiertes Fahren, Wiesbaden, Germany, October 13-14 2020.
- Christian Amersbach, Timm Ruppert, Niclas Hebgen, Hermann Winner: Macroscopic Safety Requirements for Highly Automated Driving in Urban Environments. In: 13. Graz Symposium Virtual Vehicle (GSVF), Graz, 01.-02.09.2020.
- Robert Krajewski, Michael Hoss, Adrian Meister, Fabian Thomsen, Julian Bock, Lutz Eckstein: Using drones as reference sensors for neural-networks-based modeling of automotive perception errors. In: 2020 IEEE Intelligent Vehicles Symposium (IV), Las Vegas, NV, USA, 2020, pp. 708-715, doi: 10.1109/IV47402.2020.9304615.
- Christian Neurohr, Lukas Westhofen, Tabea Henning, Thies de Graaff, Eike Möhlmann, Eckard Böde: Fundamental Arguments around Scenario-Based Testing for Automated Driving. In: 2020 IEEE Intelligent Vehicles Symposium (IV), Las Vegas, NV, USA, 2020, pp. 121-127, doi: 10.1109/IV47402.2020.9304823.
- Christian Neurohr, Lukas Westhofen, Martin Butz, Martin Bollmann, Ulrich Eberle, Roland Galbas: Criticality Analysis for the Verification and Validation of Automated Vehicles. In: IEEE Access, doi: 10.1109/ACCESS.2021.3053159.
- Maike Scholtes, Lukas Westhofen, Lara Ruth Turner, Katrin Lotto, Michael Schuldes, Hendrik Weber, Nicolas Wagener, Christian Neurohr, Martin Herbert Bollmann, Franziska Körtke, Johannes Hiller, Michael Hoss, Julian Bock, Lutz Eckstein: 6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment. In: IEEE Access, vol. 9, pp. 59131-59147, 2021, doi: 10.1109/ACCESS.2021.3072739.
- Cheng Wang, Fanglei Xiong, Hermann Winner: Reduction of Uncertainties for Safety Assessment of Automated Driving under Parallel Simulations. In: IEEE IV Transactions, 17.03.2020
- Hans Nikolaus Beck, Thomas Göppel, Stefan Specht: Begriffsmethodik zur Identifikation und Kommunikation einer Fachsprache. Überlegungen zum systematischen Erarbeiten von intentionalen fachspezifischen Begriffsregistern. 17.02.2020.

5 Abbildungsverzeichnis

Abbildung 1: Die TPs aus VVM und deren Zusammenhang 26

Abbildung 2: Die drei Arbeitsphasen in VVMethoden. 28

Abbildung 3: Übersicht der Standardisierungsaktivitäten zum automatisierten Fahren. 33

Abbildung 4: Stand der Technik, Beziehung zu Teilprojekten, Testarten und Unterkapiteln. 34

Abbildung 5: V-Modell (Prozessmodell) nach VDI-Entwicklungsmethodik für mechatronische Systeme 36

Abbildung 6: Testobjekt Gesamtfahrzeug (Darstellung aus PEGASUS, Testkonzept) 38

Abbildung 7: Testobjekt Fahrfunktion (Darstellung aus PEGASUS, Testkonzept) 39

Abbildung 8: Schematische Beispielübersicht für die systematische Absicherung am FAS-Cluster-HiL [28] 40

Abbildung 9: PEGASUS - Übersicht über das Projekt [35] 47

Abbildung 10: Aufsatzpunkt PEGASUS-Methode [35] 47

Abbildung 11: Identifikation von Automationsrisiken (Klasse 1) in [36] 48

Abbildung 12: Ein zentraler PEGASUS-Baustein: Szenario-Parameter-Datenbank [37] [38]. 49

Abbildung 13: Test- / V&V Konzept bei der Evaluierung des Risikos des ADS im Rahmen der PEGASUS-Methodik 50

Abbildung 14: Simulationsframework PEGASUS im Rahmen der Gesamtmethode [39] 51

Abbildung 15: Sicherheitsargumentation auf Basis PEGASUS-Methodik [36] [40] [41] 52

Abbildung 16: Struktur der Sicherheitsargumentation von PEGASUS [36] [40] [41]. 53

Abbildung 17: PEGASUS-Methode im V-Modell [42] 53

Abbildung 18: Überblick über die internationalen Aktivitäten von PEGASUS [35] 54

Abbildung 19: PEGASUS-Transfer: Die OpenX Standards bei ASAM [43] 55

Abbildung 20: Hintergründe der PEGASUS-Projektfamilie 55

Abbildung 21: PEGASUS Ansatz im Vergleich zu den VVM-Erweiterungen 56

Abbildung 22: Oberste Ebene der relevanten Perspektiven 57

Abbildung 23: Capability, Engineering- und Real-World-Layer der VVM-Methode 57

Abbildung 24: Vergleich PEGASUS vs. VVM-Gesamtmethode 58

Abbildung 25 - Fachliche Verbindungen VVM - ISO und UN ECE WP29 60

Abbildung 26: Übersicht über unterschiedlichen Aktivitäten auf den Gebieten Regulierung, Standardisierung, Forschungsprojekte und Datenmarktplätze. 60

Abbildung 27: V-Modell (Prozessmodell) nach VDI-Entwicklungsmethodik für mechatronische Systeme 2004 64

Abbildung 28: Beispielhafte Zerlegung des sicherheitsrelevanten (Argumentations- / Entwicklungs-) Ziels 66

Abbildung 29: Die Basis-Struktur der VVM-Gesamtmethode 67

Abbildung 30: Beispielhaft gewählte Grenzen der Testtiefe (Integrations- bzw. Systemlevel) und Testobjekte 69

Abbildung 31: V-Modell (modifizierte Darstellung) 70

Abbildung 32: Ableitung von Szenarioklassen und Szenarioinstanzen (Realitätsabstraktion) 71

Abbildung 33: Der Risk Management Core 75

Abbildung 34: Prozess zur Ableitung einer risikobasierten Verfeinerung funktionaler Spezifikationen 77

Abbildung 35: Beispielhaft gewählte Tiefe der Beschreibung der Inhalte der VVM-Methode 78

Abbildung 36: Beispielhafte Vorgehensweise zur Vermeidung von Transfer-Lücken und Divergenzen im Entwicklungsprozess 79

Abbildung 37: V-Modell (modifizierte Darstellung) mit den adventiven (Kern-) Elementen der VVM-Gesamtmethode 80

Abbildung 38: Beispielhaftes methodisches Vorgehen bei der szenariobasierten Evaluierung des Risikos 86

Abbildung 39: Ergänzungen des V-Modells durch Elemente der VVM-Gesamtmethode 88

Abbildung 40: Unterschiede zwischen der Gesamtmethode von PEGASUS (links) und VVM (rechts) 89

Abbildung 41: Überblick über die Quellen unzureichender ADS-Risikovorhersagen 90

Abbildung 42: VVM-Sicherheitsargumentationsstruktur 91

Abbildung 43: Verhältnis von Gefahren, Risiko, Sicherheitsmaßnahmen und Kriterien 91

Abbildung 44: Absicherungs-Framework - alle vier Perspektiven des Meta Layers 93

Abbildung 45: Beispiel für eine argumentative Reproduzierbarkeit der Elemente des Frameworks und der Metriken die deren Eigenschaften transferieren 94

Abbildung 46: Hauptidee: Sicherung des Speicherverhaltens bei ODD 94

Abbildung 47: links: Validierungsdreieck [52], rechts Assoziation von Argumentationskonzept und Schichten von Entwicklungsrahmen 95

Abbildung 48: Assoziation von Entwicklungsstruktur und Argumentationsstruktur 96

Abbildung 49: Vereinfachte Übersicht der argumentativen Beiträge einer Verhaltensspezifikation zur Top-Level-Argumentation 97

Abbildung 50: Eigenschaften des “Risk Management Core” (RMC) 99

Abbildung 51: Argumentation angewendet auf die Absicherung der ADS-Fähigkeiten 100

Abbildung 52:Argumentation angewendet auf die Zuverlässigkeit der Fähigkeiten des V&V Systems 101

Abbildung 53: Prozessabsicherung für die Erstellung der funktionalen Testspezifikation 101

Abbildung 54: GSN für die Dekomposition der Prozessabsicherung zur Entwicklung des V&V Systems 102

Abbildung 55: GSN für die Dekomposition der Prozessabsicherung der Testableitung und -realisierung 102

Abbildung 56: GSN für die Dekomposition der Prozessabsicherung der Testplanung 103

Abbildung 57: GSN für die Dekomposition der Prozessabsicherung der Testorchestrierung 103

Abbildung 58: Vereinfachte Darstellung der Prozesssicherungsstruktur für die Entwicklung des V&V-Systems 104

Abbildung 59: grafische Nachverfolgbarkeit zwischen Prozessen und Artefakten mit Hilfe von TRACY 105

Abbildung 60: Überblick über die Verwendbarkeit der DDI 106

Abbildung 61: Rechtliche Stakeholder bei der Zulassung automatisierter und autonomer Fahrzeuge 109

Abbildung 62: Gewichte für gefährliche Ereignisse gemäß Bußgeldkatalog 110

Abbildung 63: Schritte zur Bestimmung des quantifizierten Verkehrsverhaltens 111

Abbildung 64: Zusammenhang zwischen OD, funktionalem Anwendungsbereich und ODD 112

Abbildung 65 Abbildung 2: 6-Layer Model (6LM) als Operational-Domain-Beschreibungssprache [46] 113

Abbildung 66: Workflow Realitätsabstraktion 114

Abbildung 67: Feedbackschleifen und iteratives Konzept für die ODD-Entwicklung 114

Abbildung 68: Beispielhafte Stakeholder Anforderungen in Kombination mit möglichen Concerns als möglichen Input für die Ableitung von Top-Zielen 115

Abbildung 69: Herausforderungen bei der Ableitung von Top-Zielen 115

Abbildung 70: Unterschiedliche Hierarchieebenen von Concerns sowie ein Konflikt 116

Abbildung 71: Realitätsabstraktion im Kontext der VVM-Gesamtmethode 117

Abbildung 72: 6-Ebenen-Modell [46] zur Beschreibung eines Szenarios. 119

Abbildung 73: OD (rosa) und ODD (dunkelblau) überdeckt mit CORE-Szenarien (Waben) 121

Abbildung 74: Nutzung des ODD- Metamodells (funktionale, logische CORE Szenarien, Szenario Datenbank) im Entwicklungsprozess (V-Modell) 122

Abbildung 75: Die Rolle der CORE-Szenarien in der Gesamtmethode 124

Abbildung 76: Interdependente Reduktion von “gefährlichem Systemverhalten” 125

Abbildung 77: Abbildung 05.02.01: 6-Ebenen-Modell [46] 126

Abbildung 78: Szenarienkonzept [60] 127

Abbildung 79: Basis Szenarien (Base Scenario) aus Kombination von Konzepten [60] 128

Abbildung 80: Zusammensetzung von Verkehrsgeschehen aus Basis Szenarien als Bausteine [60] 129

Abbildung 81: Beispielhafte Parameter-Definition der Basis-Szenarien aus Kombination der Konzepte (Superclasses) [60] 130

Abbildung 82: Aufbau der Szenariodatenbank 131

Abbildung 83: Das OMEGA-Format als Schnittstelle zwischen Datenquellen und Szenario-Datenbank [60] 131

Abbildung 84: Beziehung zwischen der realen Welt, dem Szenariokonzept und der Szenariodatenbank 132

Abbildung 85: Claim „scenarios are explicitly specified" (oben in Blau) im Zusammenspiel mit der Strategie (in Gelb dargestellt) 133

Abbildung 86: Gegenargument für die in Abbildung 85 gezeigte Strategie 133

Abbildung 87: Die Automotive Urban Traffic Ontology (A.U.T.O.) 135

Abbildung 88: Prozess zur Formalisierung von Kritikalitätsphänomenen [61] 135

Abbildung 89: Netzwerk an Kritikalitätsphänomenen und ihre Relationen 136

Abbildung 90: 100 Routen im Geofence von Wolfsburg generiert 138

Abbildung 91: Links: Verteilung der erkannten Features. Mitte: Verteilung der erkannten Kritikalitätsphänomene. Rechts: Drei beispielhafte Feature Sequenzen, sortiert nach den Auftrittshäufigkeiten in den generierten Routen 139

Abbildung 92: Links: Beispielhafte Feature Sequenz entnommen aus den generierten Routen. Rechts: Kombination der Ergebnisse in einen beispielhaften Testfall gebaut in stiEF [63] angereichert mit Testanforderungen 139

Abbildung 93: Gegenüberstellung "streckenorientiert" vs. "szenario- / ereignisorientiert" 140

Abbildung 94: Scenario-based verification and Evaluation of the residual risk located in Development and safety insurance process. 141

Abbildung 95: Scenario-based verification, decomposition of the scenario-based parameter space 142

Abbildung 96: beispielhafte Zuordnung von szenariobasierten Testzielen und Methoden zur Testfallableitung aus dem Testkonzept 143

Abbildung 97: Beispielhaftes Format für eine detaillierte (technische) Testfall-Spezifikation 143

Abbildung 98: Szenariobasiertes Testen - verschiedene Merkmale / Anwendungsbereiche 144

Abbildung 99: Zielkonflikt bei der Auswahl und Priorisierung von Testfällen 145

Abbildung 100: Prozess der Ableitung von Logischen Szenarien 146

Abbildung 101: Beispiel des Hybriden Graphen der Parameter des logischen Szenarios "Merging Following Conflict" 147

Abbildung 102: Simulation-based process; search-based testing 148

Abbildung 103: Simulation-based risk assessment 149

Abbildung 104: Logisches Szenario mit fünf Szenarioparametern 149

Abbildung 105: Beispielhafte Risikobewertung des FUC2.3 für die berücksichtigten Parameter 150

Abbildung 106: Grundlegende Idee der Kritikalitätsanalyse [57] 151

Abbildung 107: Verortung der Kritikalitätsanalyse im VVM 'Assurance Framework'. 151

Abbildung 108: Übersicht zur Methodik der Kritikalitätsanalyse 153

Abbildung 109: Der Methoden-Zweig - von Assoziation zu Kausalität [57]. 154

Abbildung 110: Zeitlicher Verlauf zweier Kritikalitätsmetriken 155

Abbildung 111: Konkretisierungsschritt in der Modellierung von Wirkzusammenhängen. (© Koopmann et al. [68]) 155

Abbildung 112: Workflow zur Modellierung und Analyse von Wirkzusammenhängen 156

Abbildung 113: Effekt eines Störfaktors 157

Abbildung 114: Darstellung verschiedener minimaler Mengen von Knoten (links), die die Berechnung eines kausalen Effektes über die “Backdoor adjustment” Formel (rechts) ermöglichen 157

Abbildung 115: Vergleich angenommener Ursache-Wirkung Beziehungen 158

Abbildung 116: Beispielausschnitt aus A.U.T.O. zu Fußgängerüberwegen und Radfahrenden 159

Abbildung 117: Abstraktionsstufen der Szenarienbeschreibung 160

Abbildung 118: Ein abstraktes Kreuzungs-Szenario, vgl. [70], spezifiziert als Traffic Sequence Chart [69]. 160

Abbildung 119: Überblick der Themen des Kapitels “Fähigkeiten-Analyse und Verhaltensspezifikation” 162

Abbildung 120: Darstellung des Vorgehens bei der semantischen Normverhaltensanalyse 163

Abbildung 121: Beispielhafter PSM-Graph für ein Szenario an einer T-Kreuzung mit einem Radfahrer am Fußgängerüberweg 166

Abbildung 122: Methode zur risikobasierten Verfeinerung der Verhaltensspezifikation auf Basis des Risk Management Cores 167

Abbildung 123: Vorgehensmodell nach Reschka 170

Abbildung 124: V-Modell - ergänzt um den Vorbereitungsumfänge für korrespondierende Tests 171

Abbildung 125: Fluss der Requirements von der Anforderungsanalyse bis zur Testfall-Spezifikation 173

Abbildung 126: Requirement Flow zur Verifikation des Sicherheitskonzepts 174

Abbildung 127: Anforderungsmanagement und Anforderungs-Flow zur Test-Planung 176

Abbildung 128 Anforderungs-Flow zur Test-Orchestrierung 177

Abbildung 129 Kette der Gütemaße mit Sicherheitsbezug 179

Abbildung 130: VVM Functional Use Case "FUC2 – Straight Passing of a T-Crossing with Pedestrian Crossing“ 180

Abbildung 131 Systemanforderungen in der Nähe von Fußgängerübergängen in Bezug auf Safety 180

Abbildung 132: Fahrzeug verlangsamt, wenn es sich einem Fußgängerüberweg mit Fußgänger nähert 181

Abbildung 133: The structure of V&V within the Assurance Framework 182

Abbildung 134: Prozess-Sicht V&V im Rahmen einer scenariobasierten VVM Gesamtmethode 185

Abbildung 135: Test-Konzept 185

Abbildung 136: Fokus VVM “Systemebene” 186

Abbildung 137: Parameter-Sampling im Rahmen des szenariobasierten Testens. 187

Abbildung 138: ODD-Validierung der Vollständigkeit des ODD Metamodells 188

Abbildung 139: Schematische Darstellung des V&V Konzeptes 188

Abbildung 140: Abdeckung von V&V-Prozessen am Dekompositionsraum von ODD & Design 190

Abbildung 141: Pfad von V&V" dargestellt am Assurance Framework 191

Abbildung 142: Zusammenfassung der Beweise entlang der Argumentation 192

Abbildung 143: Testplanung im V&V-Konzept 192

Abbildung 144: Strukturierung der Testplanung 193

Abbildung 145:Testorchestrierung im V&V-Konzept 194

Abbildung 146: Testorchestrierung zur Ermöglichung „nahtlosen“ (seamless) Testens 194

Abbildung 147: Prozess der Testorchestrierung 195

Abbildung 148: Testdurchführung im V&V-Konzept 196

Abbildung 149: HiL-Testplattform für den Einfluss mechanischer Vibrationen auf die Perzeption 197

Abbildung 150: Symbiose auf Simulations- und Realtest 197

Abbildung 151: Fokus der Test Evaluation 198

Abbildung 152: Darstellung der Grundstruktur Teilprojekt TP1 199

Abbildung 153: Struktur des BOARD-Prozesses zur projektinternen Ergebnisverbreitung und Genehmigung von offiziellen VVM-Ergebnissen 199

Abbildung 154: Confluence-Dokumentation der Vorträge im Rahmen des BOARD-Prozesses. 200

Abbildung 155: Halbzeit-Event im BMW Technology Centre in München 202

Abbildung 156: Abschluss-Event in der Carl-Benz-Arena in Stuttgart 202

Abbildung 157: Zusammenspiel „Functional Use Case“ und Operational Domain/Operational Design Domain 203

Abbildung 158: Zusammenspiele unterschiedlicher Reifegrade von Kundenfunktion, ODD und technischer Implementierung 204

Abbildung 159: Strukturierung des Glossars für die technische Fachsprache, in zusätzlicher Abstimmung mit Partnerinitiativen 205

Abbildung 160: Aufbau der grafischen Benutzeroberfläche des PEGASUS-VVM-Glossars in Form eines „lebenden“ Dokuments 205

Abbildung 161: Kernaspekte der A.U.T.O.-Architektur. 215

Abbildung 162: A.U.T.O.-Architektur 215

Abbildung 163: Flussdiagramm für die Berechnung der ETM 217

Abbildung 164: Links: ax-ay Diagramm mit Höhenlinien von d_{min}, rechts: Zeitliche Entwicklung der Kritikalitätsmetriken 218

Abbildung 165: Schematische Skizze eines Zonengraphen für einen Fußgängerübergang an einer T-Kreuzung und geometrische Realisierung mit topologischem Zonengraph 219

Abbildung 166: Zwicky-Box für einen beispielhaften Entscheidungsraum 221

Abbildung 167: Szenario in Form einer Abfolge von externen Bedingungen 221

Abbildung 168: Ontologisches Modell der Entität „Kritikalitätsphänomen“ und ihrer Relationen visualisiert in VOWL 223

Abbildung 169: Modellauszug für GQM 232

Abbildung 170: Sicherheitsanalyse mit Top-Down Component Fault Tree (CFT) und Bottom-Up probFMEA 233

Abbildung 171: Ergebnisse der CFT und probFMEA Analyse hängen von der Sicht und Abstraktionsebene ab. 234

Abbildung 172: Fehlerpropagierung mit SOTIF Aspekten modelliert in safeTbox 236

Abbildung 173: Schritt 1 bis 4 der Modellierung von Fähigkeiten 237

Abbildung 174: Schematischer Ablauf des Ableitens der Testplanung aus den Systemanforderungen 238

Abbildung 175: Darstellung der Testplanung inkl. der In- und Outputs 240

Abbildung 176: Beispielhafte Funktionale Testspezifikation für die Verifikation 241

Abbildung 177: Beispielhafte Funktionale Testspezifikation für die Validierung 242

Abbildung 178: Inputs für die Testorchestrierung 243

Abbildung 179: Szenariengenerierungspipeline und wichtige Beiträge 245

Abbildung 180: a) Beispielhafte Verkehrsszenen mit fünf Fahrzeugen und sechs korrespondierenden Projektionseinheiten 246

Abbildung 181: Die Dimension des eingebundenen Raums wurde reduziert zu einem zweidimensionalen Raum unter Nutzung des UMAP-Algorithmus 246

Abbildung 182: Die AIM Forschungskreuzung (links) und der mobile Messanhänger (rechts) für mikroskopische Verkehrsmessungen und die Bereitstellung von konkreten Szenarien 249

Abbildung 183: Der Gesamtprozess zur Identifizierung und Extraktion konkreter Szenarien 249

Abbildung 184: Ein automatisch extrahiertes konkretes Szenario auf Basis einer Szenariobeschreibung 250

Abbildung 185: Schematischer Überblick über den Gesamtprozess der Kartenerstellung und Szenarienrekonstruktion. 251

Abbildung 186: Schematischer Prozess der statischen Kartenerstellung, beginnend mit der manuellen Datenauswahl entsprechend dem gegebenen Szenario. 251

Abbildung 187: Projektion (a) der generierten GT-Karte und des dynamischen Szenarios (c) auf reale Daten (b). CarMaker wird für die Simulation verwendet. 252

Abbildung 188: SACRED Methode 253

Abbildung 189: Erkannte potentiell relevante Fahrzeuge in der Vogelperspektive mit entsprechenden Kriterien und in der Ego-Ansicht 254

Abbildung 190: Links: Verfahren zur kontextbewussten Datenreduktion mit vorgeschalteter Relevanzerkennung. Rechts: A: Ursprüngliches Eingabebild, B: Reduziertes gespeichertes Bild, C: Teilweise synthetisiertes Bild 255

Abbildung 191: Datenerfassung Workflow 255

Abbildung 192: Beispiel Functional Use-Case 256

Abbildung 193: JUNCEL - Kreuzungssuche mit verschiedenen Filterkriterien 256

Abbildung 194: Referenzsensor-System Live-Viewer(links). Referenz Sensor System Setup (oben rechts), Sensor unter Test (unten rechts). 257

Abbildung 195: Digitales Logbuch mit Tags für kritische Situationen 257

Abbildung 196: Auswählen von Daten anhand von Kritikalitäts-Tags 258

Abbildung 197: Anonymisierte Videos für die visuelle Datenauswahl 258

Abbildung 198: Arbeitsablauf der Datenerfassung 259

Abbildung 199: Eingangsdatenbank für Scenario Engine 260

Abbildung 200: Konkreter Testfall in virtueller Testumgebung 260

Abbildung 201: V&V in der Gesamtmethodik 261

Abbildung 202: Testorchestrierung Detailprozess 262

Abbildung 203: Hierarchische Darstellung der Kapitel der technischen Prüfspezifikation. 264

Abbildung 204: Durchgängiges Testen 266

Abbildung 205: Technische und Funktionale Auswertung in VVM. 266

Abbildung 206: Beispiel für mehrere Ergebnisse und die Herausforderung der Aggregation. 267

Abbildung 207: Verschiedene Testplattformen und deren nahtlose Nutzung 268

Abbildung 208: Unterschiedliche Merkmale von Testplattformen 269

Abbildung 209: Vergleich verschiedener Testplattformen auf der Grundlage des Integrationsgrads. 269

Abbildung 210: Überblick über die Testmethodik-Bausteine aus VVM. 270

Abbildung 211: Cobot HiL im Betrieb 270

Abbildung 212: Sensorpositionen für Messungen in 2 m Entfernung 271

Abbildung 213: Visualisierung von Punktwolkendaten für eine Messung in 2 m Entfernung 272

Abbildung 214: Validierungsverfahren 273

Abbildung 215: Beispiel für ein logisches Szenario 275

Abbildung 216: Parameterraums mit bekannten und unbekannten sicheren Zuständen. 276

Abbildung 217: Linksabbiegeszenario mit fahrender SAE 4-Automatisierung 277

Abbildung 218: Komponenten und Abhängigkeiten des Versuchsaufbaus 278

Abbildung 219: Szenario - Linksabbiegen auf dem Testgelände 279

Abbildung 220: MoSAIC Virtual Reality Fußgängersimulator VRU mit unbegrenzter Fortbewegung 280

Abbildung 221: Augmented Reality VRU-Integration in einem Simulator 281

Abbildung 222: Beispielhafte Visualisierung eines Zebrastreifens innerhalb der VRU-Simulation 282

Abbildung 223: Open Scenario als gemeinsames Format zur Szenariobeschreibung in der Simulation und für reale Tests 283

Abbildung 224: Einsatz- und Anwendungsbereiche für eine automatisierte Testumgebung / automatisiertes Testgelände 284

Abbildung 225: ROS2-Framework zur Integration vieler Testteilnehmer in ein Testszenario 285

Abbildung 226: Entwicklungskomponenten für die Trajektorienextraktion auf Basis des ASAM OSC2.0 Standard 285

Abbildung 227: Schlechtwetterevaluationsschema für ADS. 286

Abbildung 228: Gischtgenerator, Definition des Fahrmanövers „Überholen“ und die Auswertedaten aus diesem Test. 286

Abbildung 229: Wetterkammerszenario zum lost-cargo-test und ein Bildausschnitt daraus bei Nebel mit 80m Sichtweite. 287

Abbildung 230: Kamerabilder mit über NeRFs generierter unterschiedlich starker Vernebelung (links leichter Nebel, rechts starker Nebel) 288

Abbildung 231: Abstraktionsmodell der Bewegungsmuster 288

Abbildung 232: Untersuchte makroskopische Rotationswerte für Fußgänger und Radfahrer. 289

Abbildung 233: Verteilung der Maximalwerte des Nickwinkels während der Beschleunigung für verschiedene Gangarten (links) und Verlauf von Nickwinkel, Geschwindigkeit und Beschleunigung während der Startphase 289

Abbildung 234: Untersuchte mikroskopische Bewegungswerte (links) und Platzierung der Motion Capture Sensoren. 290

Abbildung 235: Vergleich der vorderen und hinteren maximalen Hüft- und Kniewinkel von Probanden 291

Abbildung 236: Prototypische Realisierung des erweiterten Positionierungssystems und Dummy 291

Abbildung 237: Abgezielte Realfahrten-Konditionen die unter Labor-Bedingungen verlagert werden sollen 292

Abbildung 238: Abgezielte Realfahrten-Konditionen die unter Labor-Bedingungen verlagert werden sollen 293

Abbildung 239: Affinitäten der Testtechnologien in den einzelnen Aspekten des Testen der hochautomatisierten Fahrfunktion 294

Abbildung 240: Wirkkette der integrierten Testplattform und des entwickelten Wahrnehmungstestobjektes 295

Abbildung 241: Dashboard zur Analyse von Simulationsergebnissen bzgl. relevanter Parameter und Eigenschaften des zu testenden Systems 296

Abbildung 242: Instanziierung der VCIP-Referenzarchitektur mit interoperablen Werkzeugen für die systematische Bewertung hochautomatisierter Fahrfunktionen 297

Abbildung 243: Domänenmodell der maschinenlesbaren technischen Testspezifikation 298

Abbildung 244: Framework zur Testausführung 298

Abbildung 245: Konzept zum Testen hochautomatisierter Fahrzeuge in verschiedenen Testphasen 299

Abbildung 246 Überblick über den Datenfluss in VVMethoden 301

Abbildung 247 Interaktionsprozesse der Datenbankmechanik der Szenariendatenbank. 304

Abbildung 248 Screenshot einer beispielhaften Ausspielung eines Szenarios über OpenSCENARIO im Simulator esmini 305

Abbildung 249 User Interface zum Filtern und Suchen von relevanten Szenarien 306

Abbildung 250 User Interface der Perzeptionsdatenbank 307

Abbildung 251: Workflow in Coscine 308

Abbildung 252 Referenzdaten-Sensorik 309

Abbildung 253 Architektur der Sensor- und Referenz- Rohdatenbank. 310

Abbildung 254: Vorgehen zur Ermittlung von Anforderungen die aus Industriesicht eine hohe Priorität haben 313

Abbildung 255: Modellbasierte Methodik zur Aufbereitung der Workshop. 314

Abbildung 256: Metamodell in SysML zur Dokumentation und Workshopauswertung. 316

Abbildung 257: Ausschnitt aus dem mit TPX erarbeiteten Fragenkatalog. 317

Abbildung 258: Teile des Ergebnisses des Vor-Ort-Workshops 318

Abbildung 259: Exemplarische Ergebnisse verschiedener Online-Workshops 320

Abbildung 260: Überblick der Themencluster für die Priorisierung. 321

Abbildung 261: Vorgehen zur Darstellung der zu priorisierenden Anforderungen. 322

Abbildung 262: Prozessvorschlag für den Austausch mit der WG13 über das TPX und TP9. 324

Abbildung 263: VVM-Gesamtmethode – Methodenzusammenführung initiale Darstellung. 326

Abbildung 264: Initialer Prozessvorschlag zum Aufbau einer steuernden Confluence-Seite für den Ergebnisverbreitungsprozess. 328

Abbildung 265: Genereller Aufbau der Confluence-Seite zur projektinternen Ergebnisfreigabe und Dokumentation 329

Abbildung 266: Ergebnisverbreitungsprozess (projektinternes Baselining). 330

Abbildung 267: PEGASUS-Methode [36] als Prozessdarstellung mit In- und Outputs. 331

Abbildung 268: Darstellung des Informationsflusses (oben) und als „halbformale“ Prozessdarstellung (unten) in Anlehnung an SysML. 332

Abbildung 269: Generelle Struktur des Dokuments zu den Synchronisationspunkten 334

Abbildung 270: VVM-Gesamtmethode – Methodenzusammenführung 335

Abbildung 271: Modellierung der Hauptelemente der VVM-Gesamtmethode mit deren Zusammenhängen. 336

Abbildung 272: Darstellung des Zusammenhangs verschiedener Modell-/Methodenebenen. 338

Abbildung 273: Beispiel für weiterführende Zusammenhänge und Dokumentation im Modell. 340

Abbildung 274: HTML-Ausleitung des SysML-Modells, Ansicht im Browser 341

Abbildung 275: Darstellung der Inhalte aus dem SysML-Modell in verschriftlichter Form 342

Abbildung 276: Konfigurationsmanagementbereiche gemäß ISO 10007 [116]. 344

Abbildung 277: Finale Ausbaustufe des Traceability Demonstrators in VVMethoden. 345

Abbildung 278: Beispielhafte Umsetzung der Ergebnisse eines Projektmeetings in TRACY. 347

Abbildung 279: Ausschnitt der durchgängigen Argumentationskette im Teilprojekt 3 (früher Arbeitsstand im Teilprojekt). 348

Abbildung 280: Ausschnitt aus der auf dem Halbzeitevent präsentierten Umsetzung in TRACY. 349

Abbildung 281: Aufbau des Synchronisationspunktes „Capability Identification Process“ in TRACY für das Abschlussevent (finaler Softwarestand). 350

Abbildung 282: Übersicht verschiedener Darstellung und Filteroptionen in TRACY. 351

Abbildung 283: Struktur der WP.29 und GRVA. 356

Abbildung 284: Struktur der Prozesse des Masterdokuments NATM aus VMAD und der FRAV. 357

Abbildung 285: Verortung der ISO TC22 SC33 WG9 3450X Gruppen innerhalb des VVM Assurance Frameworks 360

Abbildung 286: Entwicklungszusammenhang von zur ISO TC22 SC33 WG13 TS 5083 360

Abbildung 287: zeigt schließlich weitere Standardisierungsaktivitäten und deren Verortung im VVM Assurance Framework auf. 361

Abbildung 288: Entwicklungsgeschichte der PEGASUS Expert Workshops bis zum PEW#7 "Building a robust Safety Case" 361

Abbildung 289: Key reserach topics aus der Analyse des PEW#7 "Building a robust Safety Case" 362

Abbildung 290: Globale Entwicklung und V&V-Methode 373

Abbildung 291: Szenariobasierte Entwicklung und Prüfung 374

Abbildung 292: Risikomanagement 375

Abbildung 293: Sicherheitsargumentation 376

6 Tabellenverzeichnis

Tabelle 1: TP-Leitungen 25
Tabelle 2: Allgemeine Literatur zu Ontologien 207
Tabelle 3: Terminologien im Bereich ADS 207
Tabelle 4: Ontologien aus der Automobildomäne 209
Tabelle 5: Anforderungen mit Bezug zum GQM-Modell 233
Tabelle 6: Beispiele für Simulationsanforderungen 273
Tabelle 7: Beispiel für Umgebungsmodellanforderungen 273
Tabelle 8: Beispiel für die Anforderungen an 3D-Objekte: 274
Tabelle 9: Parameter des Beispiels aus Abbildung 215 275
Tabelle 10: Die Herausforderungen des Projektes 363

7 Literaturverzeichnis

[1] VDA 2016, *Verband der Automobilindustrie e. V.,* Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems: VDA Magazin „Automatisierung – Von Fahrerassistenzsystemen zum automatisierten Fahren“, 2015; SAE J3016, 2016.

[2] W. Wachenfeld und H. Winner, *In: Autonomes Fahren, S. 439–464.,* „Die Freigabe des autonomen Fahrens“, 2015.

[3] Weiß, G.; Becker, K.; Kamphausen, B.; Radermacher, A.; Gérard, S., *Fraunhofer ESK,* "Model-driven development of self-describing components for self-adaptive distributed embedded systems": http://publica.fraunhofer.de/dokumente/N-185964.html, 2011.

[4] Weiß, G.; Grigoleit, F.; Struss, P., Kontextmodellierung für Adaption: http://publica.fraunhofer.de/dokumente/N-268926.html, 2014.

[5] DANA, „DANA – Ihre Analyseplattform für vernetzte eingebettete Systeme,“ [Online]. Available: http://www.dana.fraunhofer.de/.

[6] Weiß, G.; Schleiß, P.; Drabek, C.; Ruiz, A.; Radermacher, A., *Comprehensive Energy Management - Safe Adaptation, Predictive Control and Thermal Management, S1-18,* Safe adaptation for reliable and energy-efficient E/E architectures: http://publica.fraunhofer.de/dokumente/N-456089.html, 2017.

[7] Schleiß, P.; D., C.; Weiß, G.; Bauer, B., *Computer safety, reliability, and security. 36th International Conference, SAFECOMP 2017 : Trento, Italy, September 13-15, 2017; Proceedings, S. 179-194,* Generic management of availability in fail-operational automotive systems: http://publica.fraunhofer.de/dokumente/N-470558.html, 2017.

[8] ISO 26262, Road vehicles -- Functional safety: www.iso.org.

[9] V-Modell 97, *IABG Industrieanlagen-Betriebsgesellschaft mbH. Ottobrunn, Germany,* V-Modell 97 - komplett im Format Word (Teil 1-3)., 1997.

[10] INCOSE, *San Diego, CA, USA: International Council on Systems Engineering (INCOSE),* Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 3.2.2.: INCOSE-TP-2003-002-03.2.2., 2012.

[11] SPICE, *Verband der Automobilindustrie (VDA),* “Automotive SPICE Prozessassessment, Version 2.3”, 2007.

[12] Albers u. a., *In: ATZ elektronik (Mai 2010), S. 60–65.,* „X-in-the-Loop-Framework für Fahrzeuge, Steuergeräte und Kommunikationssysteme“., 2010.

[13] B. Schick und J. Henning, *In: 3rd Conference Active Safety through Driver Assistance. Apr. 2008,* „Simulation methods to evaluate and verify functions, quality and safety of driver assistance systems in the continuous Mil, SiL and HiL process“, 2008.

[14] Wallentowitz H. und Reif, K., Handbuch Kraftfahrzeugelektronik, 2006.

[15] H. Shokry und M. Hinchey, *In: Computer 42.4 (Apr. 2009), S. 53–59.,* „Model-Based Verification of Embedded Soft-ware“, 2009.

[16] N. Hartmann, *In: „Automatisiertes Testen Eingebetteter Systeme in der Automobilindustrie.“ München: Hanser, Carl, 2008. isbn: 9783446416352, S. 61-84,* „Test Automatisierung im Labor“, 2008.

[17] J. Schäuffele und T. Zurawka, *5. Aufl. Springer Fachmedien Wiesbaden GmbH,* Automotive Software Engineering - Grundlagen, Prozesse, Methoden und Werkzeuge effizient einsetzen, 2012.

[18] Wohlfahrt, C., et al, *6. Fachkonferenz AUTOTEST Stuttgart,* „Von Systematischer Absicherung zur ‚Digitalen Erprobungsfahrt‘“, 2016.

[19] M. Miegler u. a., *In: ATZ elektronik (Mai 2009), S. 60–65.,* „Hardware-in-the-Loop-Test von vorausschauenden Fahrerassistenzsystemen“, 2009.

[20] Bach J., Holzäpfel, M., Otten, S., Sax, E., *SAE World Congress,* Reactive-Replay Approach for Verification and Validation of Closed-Loop Control Systems in Early Development”, 2017.

[21] Conrad, Mirko, „A Systematic Approach to Testing Automotive Control Software.,“ 2004. [Online]. Available: https://www.researchgate.net/profile/Mirko-Conrad/publication/267552243_A_Systematic_Approach_to_Testing_Automotive_Control_Software/links/570cc95a08aec783ddcc6996/A-Systematic-Approach-to-Testing-Automotive-Control-Software.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcn. [Zugriff am 21 06 2024].

[22] Ference, J. J., Szabo, S., & Najm, W. G., *In 20th International Technical Conference on Enhanced Safety of Vehicles (ESV), Lyon, France, June 2007,* Objective test scenarios for integrated vehicle-based safety systems, 2007.

[23] A. Spillner und T. Linz, *Bd. 3. Heidelberg: dpunkt.verlag, 2005. isbn: 3-89864-358-1,* Basiswissen Softwaretest, 2005.

[24] E. Sax, *München: Hanser, Carl, isbn: 9783446416352 3446416358,* Automatisiertes Testen Eingebetteter Systeme in der Automobilindustrie, 2008.

[25] R. Nörenberg, *Diss. Karlsruher Institut für Technologie, isbn: 978-3-86644-842-1.,* „Effizienter Regressionstest von E/E-Systemen nach ISO 26262“, 2012.

[26] FMI, [Online]. Available: https://fmi-standard.org/. [Zugriff am 21 6 2024].

[27] Hanke, T.; Hirsenkorn, N.; van-Driesten, C.; Garcia-Ramos, P.; Schiementz, M.; Schneider, S.; Biebl, E., Open Simulation Interface: https://www.hot.ei.tum.de/forschung/automotive-veroeffentlichungen/, 2017.

[28] Ulb 2015, *S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt und M. Maurer,* Definition der Begriffe Szene, Situation und Szenario für das automatisierte Fahren.,“ Workshop Fahrerassistenzsysteme, Walting, 2015.

[29] MSC 2018, *mscsoftware.com,* Virtual Test Drive, Complete tool-chain for driving simulation applications: http://www.mscsoftware.com/product/virtual-test-drive, 2018.

[30] IPG 2018, *ipg-automotive.com,* CarMaker: Virtual testing of automobiles and light-duty vehicles: https://ipg-automotive.com/products-services/simulation-software/carmaker/, 2018.

[31] Weiskopf, M., Wohlfahrt, C., Schmidt, A., *Automotive Safety & Security,* „Integrationslösung zur Absicherung eines realen Radarsensors im Systemverbund mit der Hardware-in-the-Loop Test-technologie“, 2015.

[32] Langner, J., Bach, J., Otten, S., Sax, E., Esselborn, C., Holzäpfel, M., & Eckert, M., “Framework for using real driving data in automotive feature development and validation.”.

[33] T. Pretsch und J. Spiegel., *In: Porsche Engineering MAGAZIN 1, S. 44–51,* „Vernetzte Welt“, 2014.

[34] D. Reich u. a., *In: Interfaces 46.5, S. 409–423,* „Scheduling Crash Tests at Ford Motor Company“, 2016.

[35] T. Form, 13 05 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS_Abschlussveranstaltung_3.5_Jahre.pdf.

[36] „PEGASUS Gesamtmethode, Abschlussbericht des Projektes PEGASUS,“ [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/pdf/PEGASUS_Abschlussbericht_Gesamtprojekt.PDF und https://zenodo.org/doi/10.5281/zenodo.6595200.

[37] H. Schittenhelm, „Integration of PEGASUS tools into the certification Process," 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Symposium2019/4_4_PEGASUS_Certification_Schittenhelm.pdf.

[38] H. Schittenhelm, „PEGASUS - A Method for Assuring Safety of Conditional Automated Vehicles," in *28th Aachen Colloquium Automobile and Engine Technology*, Aachen, 2019.

[39] M. Schiementz, „Test Case Variation and Execution," 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Symposium2019/2_3_PEGASUS_TestDerivationExecution_Schiementz.pdf. [Zugriff am 21 06 2024].

[40] A. Maus, „PEGASUS Sicherheitsargumentation," 2018. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/pdf/PEGASUS Sicherheitsargumentation.pdf. [Zugriff am 21 6 2024].

[41] D. Lipinski, 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS_Abschlussveranstaltung_Wie_gut_ist_gut_genug.pdf. [Zugriff am 21 6 2024].

[42] U. Eberle, 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS_Abschlussveranstaltung_Was_brauche_ich_darueber_hinaus.pdf. [Zugriff am 21 6 2024].

[43] K. Estenfeld, 2019. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/Symposium2019/4_1_ASAM_Estenfeld.pdf. [Zugriff am 21 6 2024].

[44] W. W. H. Wachenfeld, The Release of Autonomous Vehicles, Bd. Autonomous Driving, M. G. J. L. B. W. H. Maurer, Hrsg., Springer, Berlin, Heidelberg, 2016.

[45] N. W. e. al., „A simulation based, statistical approach for the derivation of concrete scenarios for the release of highly automated driving functions," in *11th GMM Symposium, Dortmund, Germany*.

[46] M. Scholtes, L. Westhofen, L. R. Turner, K. Lotto, M. Schuldes, N. Wagener, C. Neurohr, M. H. Bollmann, F. Körte, J. Hiller, M. Hoss, J. Boch, L. Eckstein und H. Weber, „6-Layer Model for a Structured Description and Categorization of Urban Traffic and Environment".*IEEE Access.*

[47] „VVM Projekt," 21 6 2024. [Online]. Available: https://www.vvm-projekt.de/fileadmin/user_upload/VVM_Glossar_V4_20231109_de.pdf.

[48] ISO 21448: Road vehicles -- Safety of the intended functionality, Geneva: International Organization for Standardization, 2022.

[49] „https://bmdv.bund.de/," 2017. [Online]. Available: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile. [Zugriff am 21 6 2024].

[50] N. F. Salem und et al., „Risk Management Core—Toward an Explicit Representation of Risk in Automated Driving," *IEEE Access,* Bd. 12, p. 33200–33217, 2024.

[51] C. Glasmacher und L. Eckstein, „https://arxiv.org/," 2024. [Online]. Available: https://arxiv.org/pdf/2404.01934. [Zugriff am 21 6 2024].

[52] J. E. Stellet, T. Brade, A. Poddey, S. Jesenski und W. Branz, „Formalisierung und algorithmischer Ansatz zur Validierung des automatisierten Fahrens," 2019.

[53] ISO 16290 2013, *Beuth,* Raumfahrtsysteme - Definition des Technologie-Reifegrades (TRL) und der Beurteilungskriterien: http://www.beuth.de/de/norm-entwurf/din-iso-16290/224384199, 2013.

[54] E. Armengaud und et al., „DEIS: Dependability Engineering Innovation for Industrial CPS".*Advanced Microsystems for Automotive Applications.*

[55] 202104, Hrsg., „Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," in *SAE International Standard J3016*, 2021.

[56] B. d. Justiz, „Straßenverkehrs-Ordnung," [Online]. Available: https://www.gesetze-im-internet.de/stvo_2013/index.html. [Zugriff am 21 6 2024].

[57] C. Neurohr, L. Westhofen, M. Butz, M. H. Bollmann, U. Eberla und R. Galbas, „Criticality Analysis for the Verification and Validation of Automated Vehicles," *IEEE Access,* Bd. 9.

[58] H. Weber, C. Glasmacher, M. Schuldes, N. Wagener und L. Eckstein, „Holistic Driving Scenario Concept for Urban Traffic," *IEEE Symposium on Intelligent Vehicle,* 2023.

[59] OMEGA Format, „https://github.com/," [Online]. Available: https://github.com/ika-rwth-aachen/omega_format.

[60] C. Glasmacher, M. Schuldes, P. Topalakatti, P. Hristov, H. Weber und L. Eckstein, „Deliverable 13 - Scenario-based Model of the ODD through Scenario Databases".

[61] A. Wellßow, *Entwurf eines Prozesses zur Formalisierung sicherheitsrelevanter Phänomene für das automatisierte Fahren,* 2022.

[62] L. Westhofen und et al., *Answering Temporal Conjunctive Queries over Description Logic Ontologies for Situation Recognition in Complex Operational Domains,* TACAS'24, Luxembourg, 2024.

[63] F. Bock und J. Lorenz, „Abstract Natural Scenario Language Version 1.0," in *Technical Disclosure Commons*, 20.09.2022.

[64] C. Neurohr, L. Westhofen, M. Butz, M. H. Bollmann, L. Putze, T. Kooopmann, R. Gansch, M. Knoop, A. Rasch, B. Cojocaru und J. Daube, „Advances on the Criticality Analysis for Automated Driving Systems".

[65] L. Westhofen, C. Neurohr und T. Koopmann, „Criticality Metrics for Automated Driving: A Review and Suitability Analysis of the State of the Art," *Archives of Computational Methods in Engineering 30,* pp. 1-35, 2023.

[66] S. Babisch, C. Neurohr, L. Westhofen, S. Schoenawa und H. Llers, „Leveraging the GIDAS Database for the Criticality Analysis of Automated Driving Systems," *Journal of Advanced Transportation,* 2023.

[67] L. Westhofen, C. Neurohr, M. Butz, M. Scholtes und M. Schuldes, *Using ontologies for the formalization and recognition of criticality for automated driving,* IEEE OJITS, 2022.

[68] C. Koopmann, C. Neurohr, L. Putze, L. Westhofen, R. Gansch und A. Adee, „Grasping Causality for the Explanation of Criticality for Automated Driving," 2022.

[69] J. S. Becker, T. Koopmann, B. Neurohr, C. Neurohr, L. W. Westhofen, E. Böde und W. Damm, „Simulation of Abstract Scenarios: Towards Automated Tooling in Criticality Analysis," *Autonomes Fahren. Ein Treiber zukünftiger Mobilität,* 2022.

[70] C. Neurohr, L. Westhofen, T. Duong Quang, T. Koopmann, R. Gansch und S. Schoenawa, „Deliverable 09 - Requirements on Simulation Systems and Models Posed by a Criticality Analysis for Automated Driving Systems," VVM Projekt.

[71] N. F. Salem, V. Haber, M. Rauschenbach, M. Nolte, J. Reich, T. Stolte, R. Graubohm und M. Maurer, *Ein Beitrag zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge,* arXiv, 2022.

[72] H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach und J. Reich, *Phänomen-Signal-Modell: Formalismus, Graph und Anwendung,* arXiv, 2021.

[73] H. N. Beck, N. F. Salem, V. Haber, M. Rauschenbach und J. Reich, *Phenomenon-Signal Model: Formalisation, Graph and Application,* arXiv, 2022.

[74] T. Menzel, G. Bagschik und M. Maurer, „Scenarios for Development, Test and Validation of Automated Vehicles," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018.

[75] G. Bagschik, T. Menzel, A. Reschka und M. Maurer, „Szenarien für Entwicklung, Absicherung und Test von automatisierten Fahrzeugen," in *11. Workshop Fahrerassistenzsysteme*, Walting im Altmühltal, 2017.

[76] N. F. Salem, T. Kirschbaum, M. Nolte, C. Lalitsch-Schneider, R. Graubohm, J. Reich und M. Maurer, *Risk Management Core – Towards an Explicit Representation of Risk in Automated Driving,* arXiv, 2023.

[77] A. Reschka, G. Bagschik, S. Ulbrich, M. Nolte und M. Maurer, „Ability and Skill Graphs for System Modeling, Online Monitoring, and Decision Support for Vehicle Guidance Systems," in *2015 IEEE Intelligent Vehicles Symposium (IV)*, 2015.

[78] M. Nolte, G. Bagschik, I. Jatzkowski, T. Stolte, A. Reschka und M. Maurer, „Towards a Skill- And Ability-Based Development Process for Self-Aware Automated Road Vehicles," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, 2017.

[79] G. Bagschik, M. Nolte, S. Ernst und M. Maurer, „A System's Perspective Towards an Architecture Framework for Safe Automated Vehicles," in *2018 IEEE International Conference on Intelligent Transportation Systems (ITSC)*, 2018.

[80] T. Stolte, R. Graubohm, I. Jatzkowski, M. Maurer, S. Ackermann, B. Klamann, M. Lippert und H. Winner, „Towards Safety Concepts for Automated Vehicles by the Example of the Project UNICARagil," in *29th Aachen Colloquium Sustainable Mobility 2020*, 2020.

[81] R. Graubohm, T. Stolte, G. Bagschik und M. Maurer, „Towards Efficient Hazard Identification in the Concept Phase of Driverless Vehicle Development," *2020 IEEE Intelligent Vehicles Symposium (IV),* p. 1297–1304, October 2020.

[82] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle und W. Damm, „Identification and Quantification of Hazardous Scenarios for Automated Driving," in *Model-Based Safety and Assessment*, Bd. 12297, M. Zeller und K. Höfig, Hrsg., Cham, Springer International Publishing, 2020, p. 163–178.

[83] D. Fowler, „IEC 61508 Viewpoint on System Safety in the Transport Sector: Part 1–An Overview of IEC 61508," *Safety-Critical Systems eJournal,* Bd. 1, 2022.

[84] G. Bagschik, „Systematischer Einsatz von Szenarien für die Absicherung automatisierter Fahrzeuge am Beispiel deutscher Autobahnen," Braunschweig, 2022.

[85] A. Reschka, „Fertigkeiten- und Fähigkeitengraphen als Grundlage des sicheren Betriebs von automatisierten Fahrzeugen im öffentlichen Straßenverkehr in städtischer Umgebung," 2017.

[86] C. S. Sippl, 2020. [Online]. Available: https://opus4.kobv.de/opus4-fau/frontdoor/index/index/docId/15023. [Zugriff am 13 3 2023].

[87] ISO/IEC 19540:2022, *Information technology — Object Management Group Unified Architecture Framework (OMG UAF),* International Organization for Standardization, 2022.

[88] T. Report, „Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation," International Organization for Standardization, Geneva, 2020.

[89] C. S. Wasson, System engineering analysis, design, and development: concepts, principles, and practices, Hoboken, New: John Wiley & Sons Inc, 2015.

[90] B. d. Justiz, „Gesetz über die Haftung für fehlerhafte Produkte," [Online]. Available: https://www.gesetze-im-internet.de/prodhaftg/. [Zugriff am 21 6 2024].

[91] *Richtlinien für die Anlage und Ausstattung von Fußgängerüberwegen (R-FGÜ 2001) vom Bundesministerium für Verkehr, Bau und Wohnungswesen,* 2001.

[92] M. Butz, C. Heinzemann, M. Herrmann, J. Oehlerking, M. Rittel, N. Schalm und D. Ziegenbein, „SOCA: Domain Analysis for Highly Automated Driving Systems".

[93] N. F. Salem, V. Haber, M. Nolte, R. Graubohm, M. Rauschenbach, J. Reich, T. Stolte und M. Maurer, „Semantische Normverhaltensanalyse zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge," Berkheim, 2023.

[94] V. R. Basili, G. Caldiera und H. D. Rombach, „Goal Question Metric Paradigm," in *Encyclopedia of Software Engineering - 2 Volume Set*.

[95] M. Rauschenbach, S. Kupjetz, C. Wolschke und T. Braun, „Ansatz zur methodischen Analyse und Absicherung des Funktionalkonzepts voll automatisierter Kraftfahrzeuge," 2021.

[96] J. Pott, M. Rauschenbach, M. Mai, T. Braun, S. Kupjetz und C. Wolschke, „An Approach for Decomposition and Analysis," 2022.

[97] M. Zipfl und J. M. Zöllner, „Towards Traffic Scene Description: The Semantic Scene Graph," *IEEE 25th International Conference on Intelligent Transportation Systems (ITSC),* pp. 3748-3755, 2022.

[98] M. Zipfl, M. Jarosch und J. M. Zöllner, „Self Supervised Clustering of Traffic Scenes using Graph Representations," *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME),* pp. 1-7, 2022.

[99] M. Zipfl, M. Jarosch und J. M. Zöllner, „Traffic Scene Similarity: a Graph-based Contrastive Learning Approach".

[100] M. Zipfl, S. Spickermann und J. M. Zöllner, „Utilizing Hybrid Trajectory Prediction Models to Recognize Highly Interactive Traffic Scenarios," *26th IEEE International Conference on Intelligent Transportation Systems ITSC,* 2023.

[101] M. Zipfl, B. Schütt, J. M. Zöllner und E. Sax, „Fingerprint of a Traffic Scene: an Approach for a Generic and Independent Scene Assessment," *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME),* 2022.

[102] M. Höfer, F. Fuhr, B. Schick und P. E. Pfeffer, „Attribute-based development of driver assistance systems," *10th International Munich Chassis Symposium,* 2019.

[103] D. Schneider, B. Huber, H. Lategahn und B. Schick, „Measuring method for function and quality of automated lateral control based on high-precision digital "Ground Truth" maps," *VDI/VW-Gemeinschaftstagung Fahrerassistenzsysteme und Automatisiertes Fahren,* 2018.

[104] S. Keidler, J. Haselberger, K. Mayannavar, B. Schick und D. Schneider, „Development of lane-precise "Ground Truth" maps for the objective Quality Assessment of automated driving functions," *VDI Reifen – Fahrwerk – Fahrbahn,* 2019.

[105] K. Mori, K. Storms und S. Peters, „Conservative Estimation of Perception Relevance of Dynamic Objects for Safe Trajectories in Automotive Scenarios".

[106] K. Storms, K. Mori und S. Peters, „SURE-Val: Safe Urban Relevance Extension and Validation," [Online]. Available: https://arxiv.org/abs/2308.02266?context=cs.

[107] M. Fischer, G. Temme, K. Gröne, D. Martinez Garcia, G. Grolms und J. Rehm, „A VRU-simulator for the evaluation of pedestrian- and cyclist-vehicle interaction – Design criteria and implementation," in *Proceedings of the Driving Simulation Conference Europe*, Straßbourg, France, 2022.

[108] A. Bachorek, I. Mironov und M. Meiler, „A Virtual Testbed for Detecting Feature Interactions in ADAS/AD Function Design," *22nd Driving Simulation & Virtual Reality Conference & Exhibition,* 2023.

[109] A. Bachorek und J. Jung, „Establishing Virtual Test-Driven Development Environments in the Automotive Domain : A Continuous Engineering Approach," *11th IEEE/ACM Int. Workshop on Software Engineering for Systems-of-Systems and Software Ecosystems,* 2023.

[110] H. Gremmelmaier und L. Hierzegger, „Cyclist's behavior: a survey on characteristics and trajectory modeling," *26th IEEE International Conference on Intelligent Transportation Systems ITSC,* 2023.

[111] F. Mütsch, H. Gremmmelmaier, N. Becker, D. Bogdoll, M. R. Zofka und J. M. Zöllner, „From Model-Based to Data-Driven Simulation: Challenges and Trends in Autonomous Driving," *Workshop Vision-Centric Autonomous Driving (VCAD), CVPR,* 2023.

[112] M. R. Zofka, T. Fleck und J. M. Zöllner, „A Unified Description of Proving Grounds and Test Areas for Automated and Connected Vehicles," *2022 IEEE Intelligent Vehicles Symposium (IV),* pp. 1430-1437, 2022.

[113] M. R. Zofka, T. Fleck, P. Schörner, M. Heinrich und J. M. Zöllner, „Paving the Ways for Vehicles-in-the-loop: Wireless Integration of Autonomous Vehicles into Mixed Reality Proving Grounds and Test Areas," *26th IEEE International Conference on Intelligent Transportation Systems ITSC,* 2023.

[114] B. Deutschland, „Strategie automatisiertes und vernetztes Fahren," [Online]. Available: ttps://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/broschuere-strategie-automatisiertes-vernetztes-fahren.pdf?__blob=publicationFile.

[115] PROSTEP2015, „Hans-Martin Heinkel, Martin Geissen (interne Projektpräsentation)," Smart Systems Engineering Status & next Steps WP2, SmartSE Check, 2015.

[116] D. G. f. Qualität, „DIN ISO 10007:2020-10," [Online]. Available: https://www.dgq.de/skripts/aktiv/gf_asset_proxy.php?i=42254&h=9420072e27236065a43b721423fe086bdba0ec01&n=10007_Konfigurationsmanagement_Hampe.pdf&c=application%2Fpdf. [Zugriff am 21 6 2024].

[117] P. Mäder und A. Egyed, „Do Developers Benefit from Requirements Traceability When Evolving and Maintaining a Software System?," in *Empirical Software Engineering*, 2015.

1 ANNEX I - VVM Position Papier

1.1 Introduction

1.1.1 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 [2] 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.

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

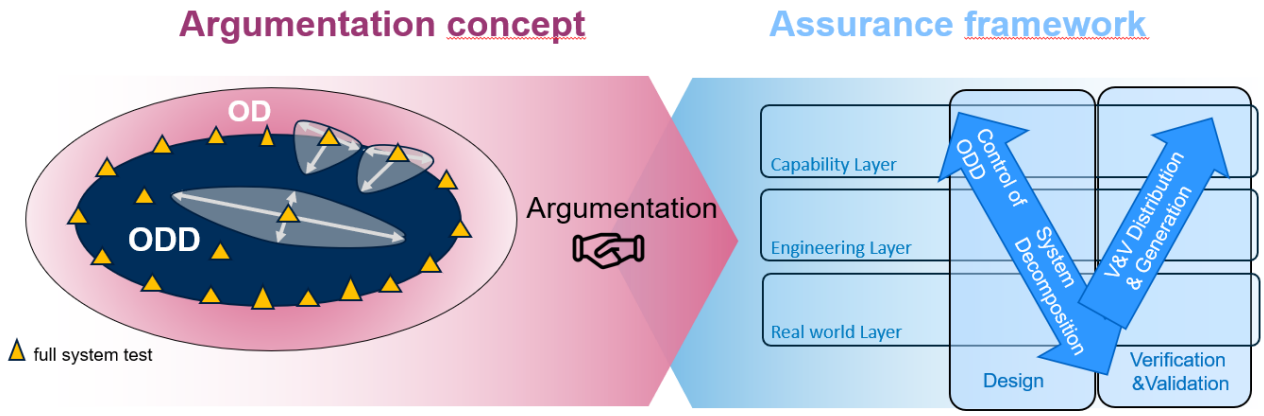


Figure 1: Overall VVM design space: Argumentation concept and assurance framework

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 1.1.

Chapter 1.2 presents and discusses the main VVM position towards a central VVM thesis statement and four subtheses with related argumentations, see Figure 2. Overall VVM design space: Argumentation concept and assurance framework. 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.

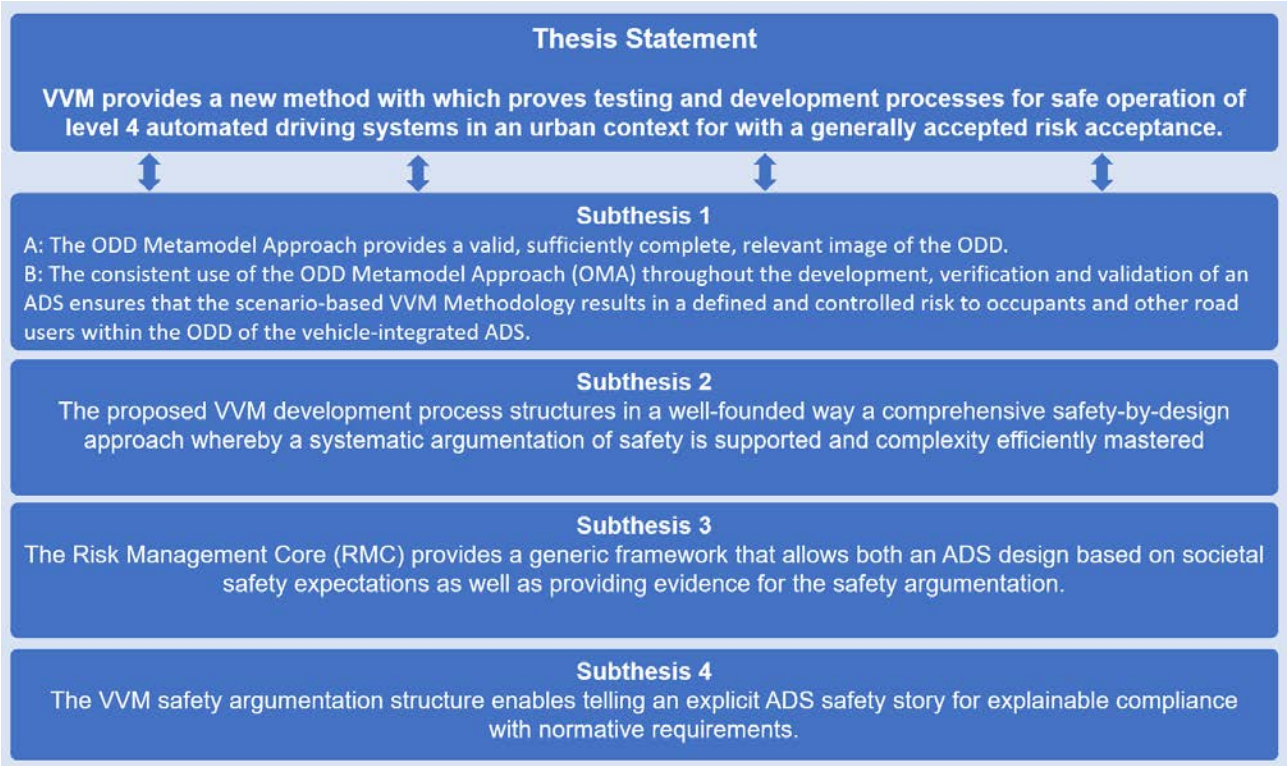


Figure 2: VVM general thesis statement and according subtheses

In Chapter 1.3 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 1.4, supplemented by recommendations how scenario-based testing methodologies can be applied.

1.1.2 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

1.1.3 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.

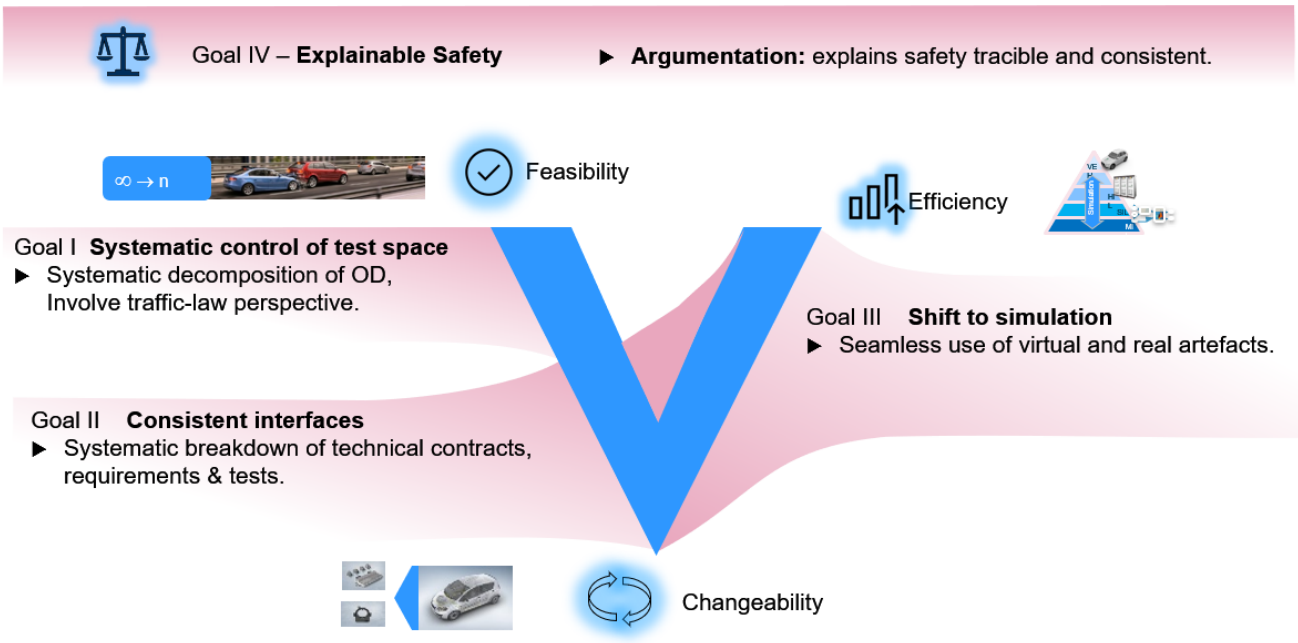


Figure 3: VV Methods management top goals of project

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.

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.

1.2 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.

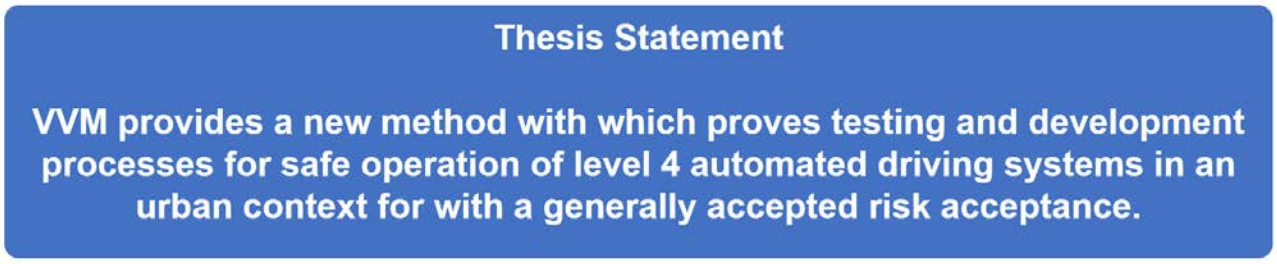


Figure 4: General thesis statement

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.

1.2.1 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.

1.2.2 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".

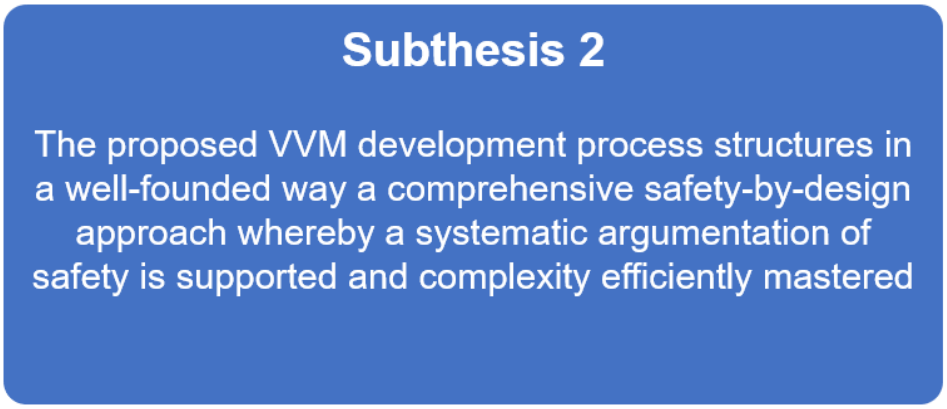


Figure 6: Subthesis 2

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.

1.2.3 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 1.1.3 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.

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.

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

1.2.4 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**.

1.3 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.

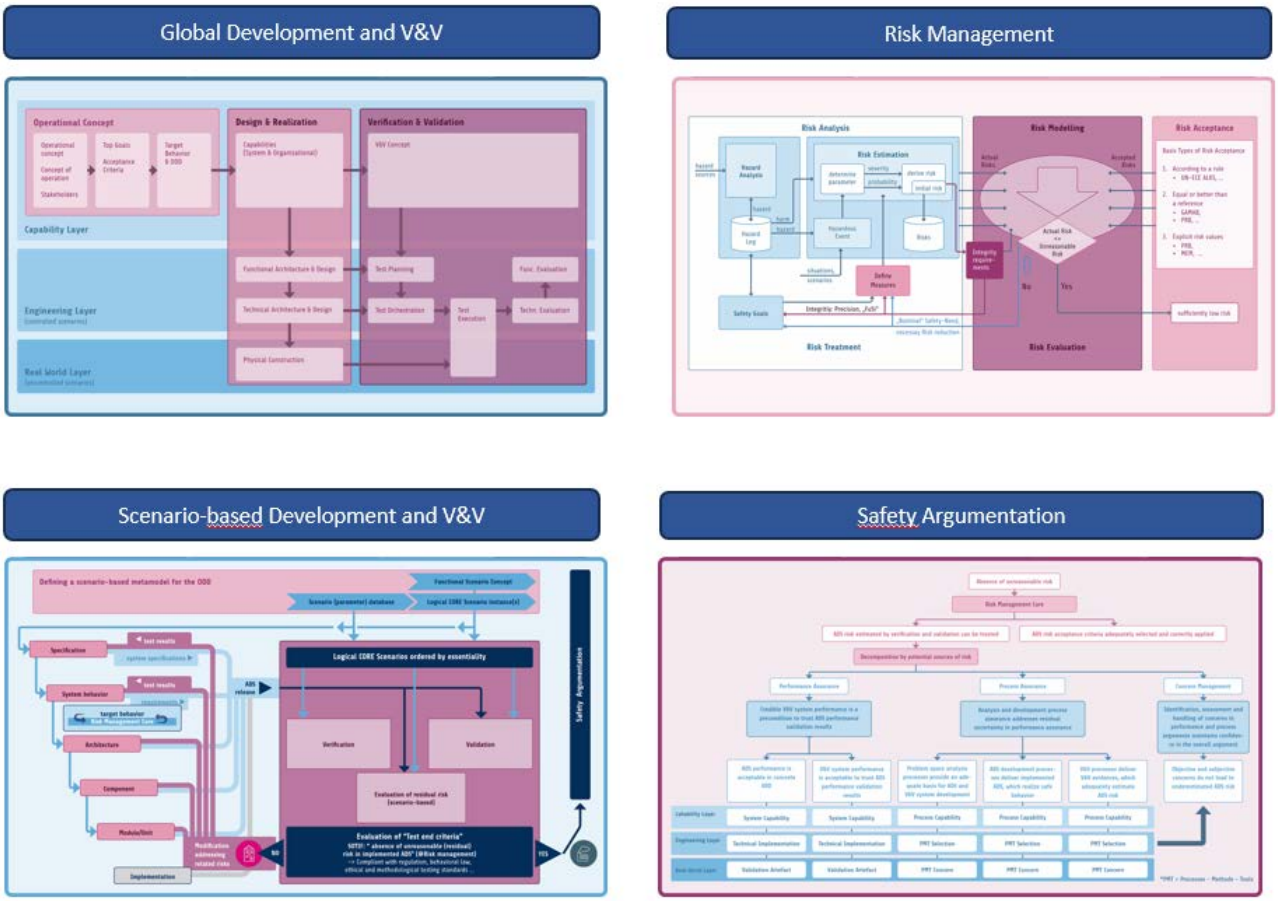


Figure 9: Four methodological processes to reach the goal: Assurance of a **safe** AD System by demonstrating the absence of **unreasonable risk**

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.

1.3.1 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).

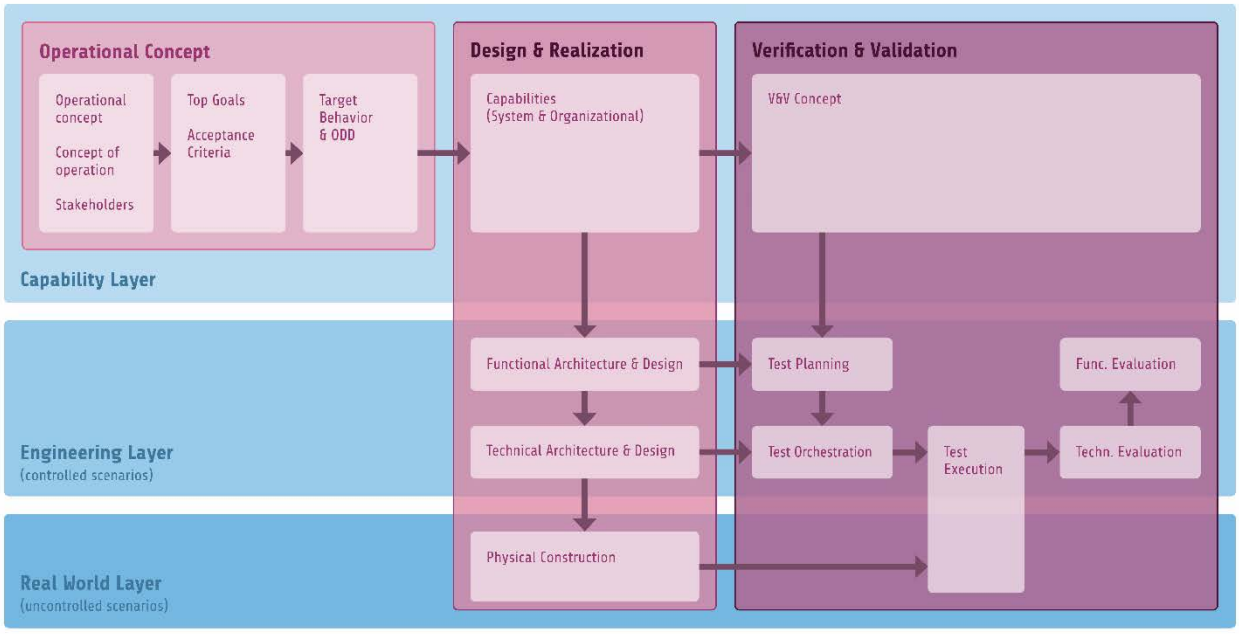


Figure 10: Global Development and V&V method

- 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".

1.3.2 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.

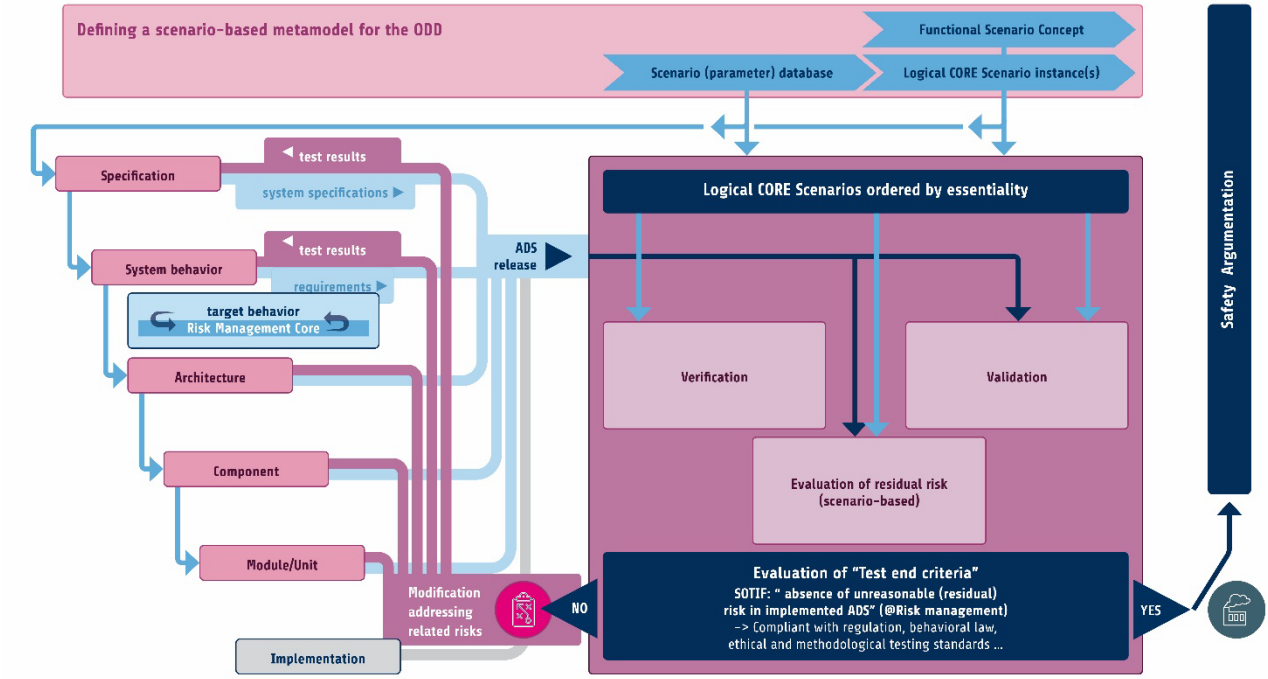


Figure 11: Scenario-Based Testing and Development method

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.

1.3.3 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.

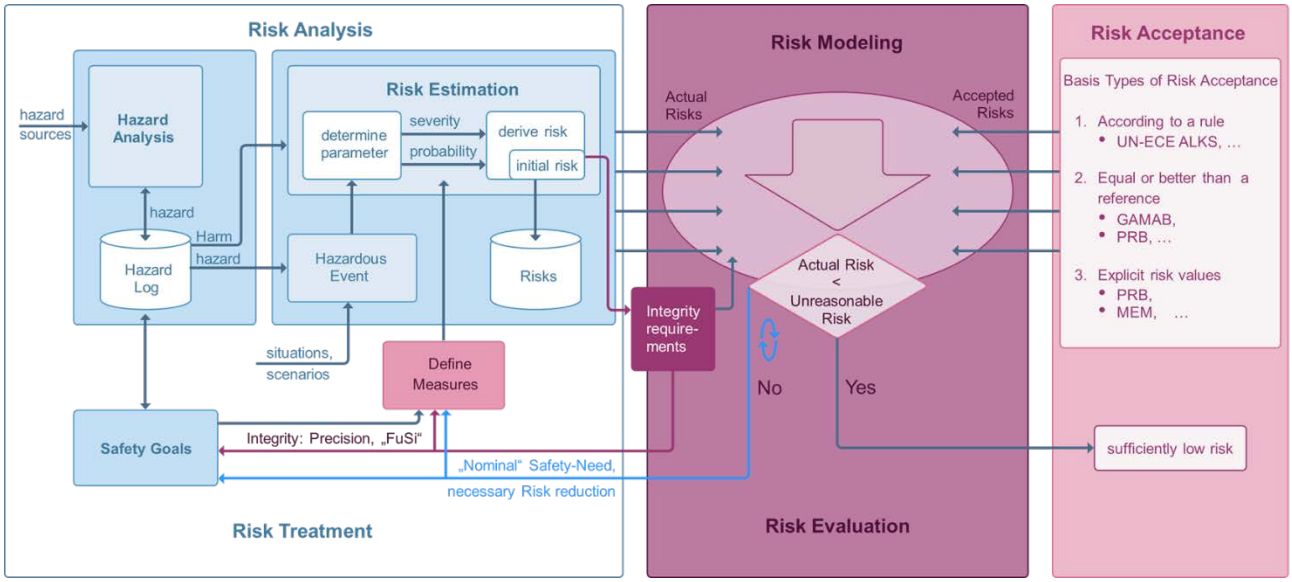


Figure 12: The Risk Management Core method

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 1.1.3 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".

1.3.4 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.

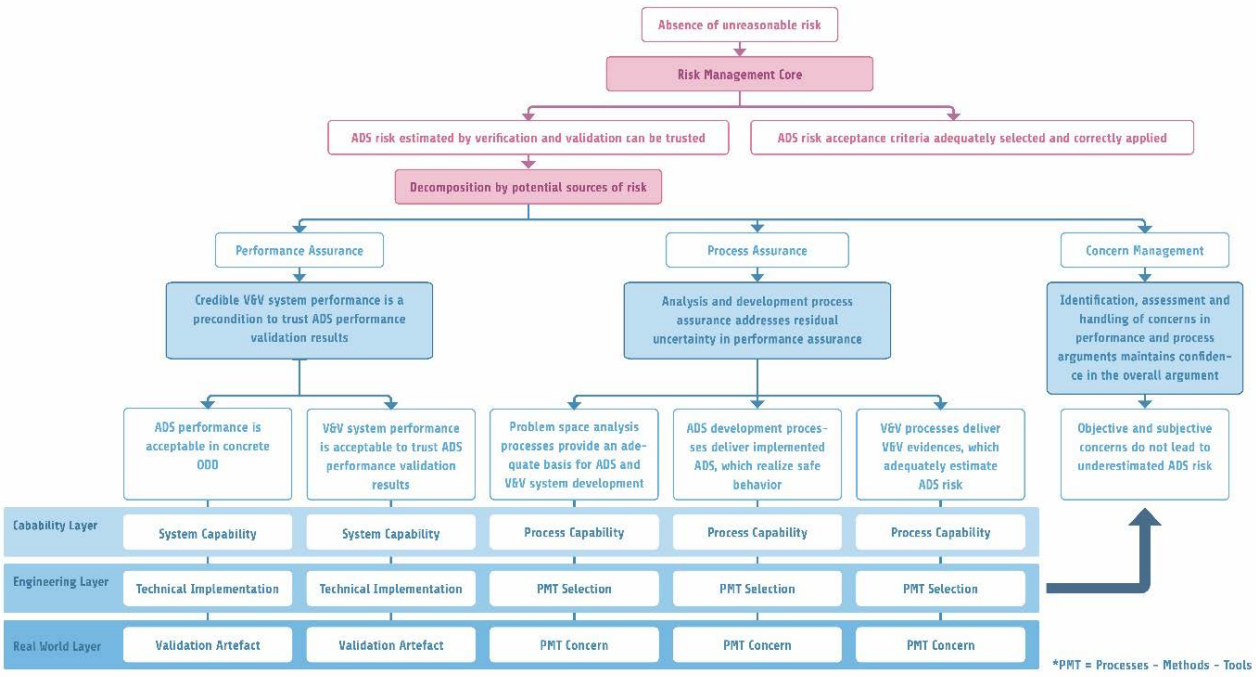


Figure 13: The VVM Safety Argumentation structure method

1.3.5 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.

1.4 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.

1.4.1 Outlook: Scenario-based testing and virtualization

1.4.1.1 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.

1.4.1.2 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.

1.4.1.3 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.

1.4.1.4 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

1.4.1.5 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.

1.4.2 Outlook: Risk Handling and safety case application

1.4.2.1 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[3], 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.

1.4.2.2 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).

[3] 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.

1.4.2.3 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.

1.4.3 Outlook: Technological Challenges

1.4.3.1 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 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.

1.4.3.2 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.

1.4.3.3 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.

1.4.3.4 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.

1.4.3.5 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.

1.5 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.