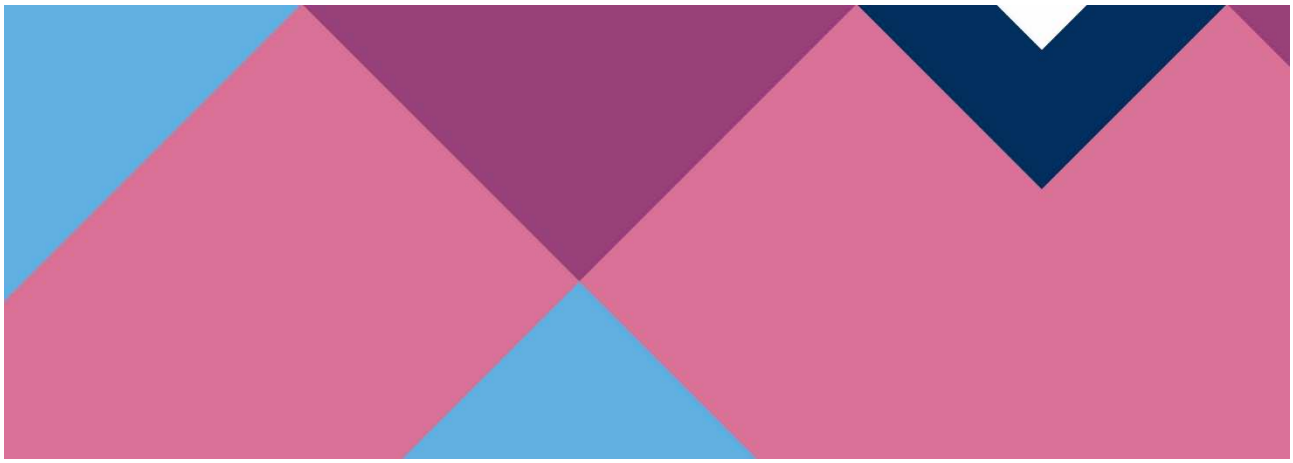
VERIFICATION
VALIDATION
METHODS

VVM - Schlussbericht

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



Version 1.0 Final

Zuwendungsempfänger Fraunhofer Gesellschaft

Förderkennzeichen 19A19002K

Laufzeit des Vorhabens 07/2019 - 12/2023

PEGASUS
FAMILY

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Dokumenteninformation

Autoren

Jürgen Nuffer, LBF

Matthias Rauschenbach, LBF

Simon Kupjetz, LBF

Jonathan Millitzer, LBF

Jan Reich, IESE

Daniel Hillen, IESE

Joshua Frey, IESE

Martin Urban, IVI

Dominik Schreiber, IVI

Kontakt

Dr. Jürgen Nuffer
Gruppenleiter Zuverlässigkeit und Sicherheit aktiver Systeme
Abteilung Strukturdynamik und Schwingungstechnik
Bereich Adaptronik
Fraunhofer-Institut für Betriebsfestigkeit und Systemzuverlässigkeit LBF
Bartningstrasse 47
64289 Darmstadt

Tel. +49 - (0)6151 - 705 281
mobil +49 - (0)172 - 6114645

juergen.nuffer@lbf.fraunhofer.de

Inhaltsverzeichnis

0 Kurzdarstellung

0.1 Aufgabenstellung

Die Fraunhofer Gesellschaft war am Projekt mit drei Instituten (LBF, IESE, IVI) beteiligt. Im Gesamtprojekt war das wesentliche Ziel die Entwicklung von Systematik und Methoden für den Sicherheitsnachweis von vollautomatisierten und fahrerlosen Fahrfunktionen und Fahrzeugen (Level 4/5 nach VDA-Definition zur Homologation im urbanen Umfeld.

Die FhG mit ihren beteiligten Instituten hat hierbei das Teilprojekt „Sicherheitskonzept und Ableitung von System- und Testanforderungen“ bearbeitet. Die FhG verfolgte in VVM folgende Aufgaben:

- Unterstützung bei der methodischen Entwicklung der Sicherheitsanalyse mithilfe der probabilistischen FMEA (in Kombination mit Component Fault Trees)
- Erarbeitung eines methodischen Frameworks zur Ableitung von System- und Testanforderungen
- Unterstützung bei der Zusammenstellung des Stands der Technik mit Fokus auf das Testen mechatronischer Systeme; Hierarchisierung, Priorisierung und Strukturierung von Anforderungen
- Bewertung von Testmitteln und Testrergebnissen; Konzeptionierung von Testinfrastrukturen unter Einbringung der Kompetenzen im Bereich XiL-Testumgebungen
- Praktische Umsetzung und Anwendung einer XiL-Testumgebung
- Entwicklung von Methoden zur Entwicklung hochzuverlässiger und sicherheitskritischer softwareintensiver eingebetteter Systeme
- Anpassung und Integration von Methoden und Ergebnissen aus PEGASUS zur Validierung und Verifikation eines Safety Supervisors,
- Erstellung modellbasierter Spezifikationen mit dem hauseigenen safety engineering Tool SafeTbox,
- Untersuchung und Strukturierung der Methodik mittels der Goal Structuring Notation (GSN).
- Erhebung kritischer und typischer Verkehrssituationen an Knotenpunkten mittels infrastrukurbasierter Messtechnik
- Bestimmung der Knotenpunkte, an denen die Messtechnik zu installieren ist. Die dort aufgezeichneten Videos sind mithilfe bildverarbeitender Algorithmen zu analysieren, sodass im Ergebnis Trajektorien und Geschwindigkeiten der Verkehrsteilnehmer zur Verfügung gestellt werden.

0.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

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.

0.3 Planung und Ablauf des Vorhabens

Das Projekt folgte im wesentlichen der ursprünglichen Planung, was die Abfolge und Bearbeitung der in der VHB festgelegten Ergebnisse betrifft.

Insgesamt wurden seitens der Projektleitung zur besseren Durchführung und Interaktion der Partner übergreifende Arbeitsgruppen (tlw. auch als „Schnellboot“ und „Core“-Gruppen bezeichnet) gebildet, die sich spezifischen Fragestellungen widmete. Die FhG war hier insbesondere in allen Arbeitsgruppen beteiligt, die im Umfeld der TP3, 4, und 7 angesiedelt waren.

Während des gesamten Projekts wurden die Aufwände planmäßig abgerufen, auch wenn ursprünglich geplante Reisemittel aufgrund der COVID-19-Pandemie zunächst nicht verwendet wurden. Im Halbjahr 2/2020 wurde auf Gesamtprojektebene die Wichtigkeit einer projektübergreifenden Sicherheitsargumentation festgestellt, die in dieser Form nicht geplant war. Aufgrund der Kompetenz und Vorarbeiten in diesem Bereich hat das IESE die Verantwortung über die Koordination der Sicherheitsargumentation in der Core03-Gruppe übernommen, was zu einer Verlagerung der Aufwände führte, die ursprünglich für die Integration des dynamischen Risikomanagements vorgesehen waren. Diese Verlagerung der Aufgaben wurde mit den Projektkoordinatoren abgestimmt und als entscheidend für die Gesamtprojektziele erachtet.

Trotz personeller Engpässe und der Notwendigkeit zusätzlicher Ressourcen konnte das IESE durch den verstärkten Einsatz von studentischen Hilfskräften und die Umwidmung von ungenutzten Reisemitteln sicherstellen, dass keine Verzögerungen bei den Ergebnissen auftraten. Die koordinierten Anstrengungen im Rahmen von Core03 und die fortlaufende Anpassung der Methodik haben die Grundlage für die Sicherheitsargumentation und die Einbindung in das Assurance Framework gestärkt. Covid-induzierte Verzögerungen wurden durch die kostenneutrale Verlängerung um ein halbes Jahr aufgefangen.

Die Erzeugung der IESE-Beiträge zur probFMEA-CFT Methodik in TP4 sowie zur modellbasierten Sollverhaltensspezifikation in TP3 folgten im wesentlichen der Planung in der Vorhabensbeschreibung.

0.4 Stand der Wissenschaft und Technik, an den angeknüpft wurde

Zum Zeitpunkt der Antragstellung waren im Homologationsprozess für L4/5 Fahrzeuge verschiedene Defizite im Stand von Wissenschaft und Technik identifiziert worden, an die angeknüpft wurde. L4/L5-Systeme agieren per Konstruktion selbständig („intelligent“) in Situationen, die bei der Entwicklung der Systeme nicht explizit berücksichtigt wurden. Ihre Verhaltensgrenzen sind dabei nicht genau bekannt und somit fehlt 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 beschäftigen sich mit dieser Problematik. Alle Lösungen haben gemeinsam, dass sie versuchen, das Risiko bezüglich ganz allgemeiner Unfallarten zur Laufzeit zu bestimmen und zu kontrollieren, wobei ein dynamisches Risikomanagement anwendungsdomänenübergreifend im Kontext von Avionik, Robotik, und Automotive vorgeschlagen wurde. Dieses Risikomanagement muss dabei auch in den System- und Testanforderungen berücksichtigt werden.

Die Normvorgaben der ISO 26262 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 umfasst 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 wirft eine Reihe von Fragestellungen bezüglich der Herangehensweise zur Erfüllung der Normanforderungen auf.

Die Normung zur funktionalen Sicherheit und die darauf bezogene praktische Umsetzung beziehen sich in Ihrem heutigen 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 wird 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“ erweitert damit nicht nur den nach ISO 26262 abzusichernden Funktionsumfang erheblich, sondern fügt grundsätzlich neue funktionale Aspekte hinzu. Deren Absicherung durch systematische Testfallableitung, Testspezifikation und -umsetzung ist bisher in der Praxis und der zugrundeliegenden Normung nicht thematisiert.

Fraunhofer baute im Projekt auf dem Stand der Wissenschaft und Technik im Bereich der Entwicklung hochzuverlässiger und sicherheitskritischer softwareintensiver eingebetteter Systeme auf. Die Entwicklung der probFMEA/CFT Methodik basierte auf der am IESE seit vielen Jahren entwickelten Component Fault Tree (CFT) Methode zur Sicherheitsanalyse und der am LBF bereits in anderen Themenbereichen angedachten probabilistischen FMEA. Modellbasierte Spezifikationen wurden mithilfe des eigenen Tools SafeTbox und dem Technology Stack rund um „Digital Dependability Identities“ erstellt, der durchgängig nachverfolgbare tool-unabhängige Safety-Modelle

ermöglicht. Zur Modellierung der VVM Sicherheitsargumentation kam die etablierte Goal Structuring Notation (GSN) zum Einsatz. Auf Basis bestehender Forschungsergebnisse, insbesondere der Forschungsprojekte mit den Schwerpunkten Safety, Verifikation/Validierung und Sicherheitsargumentationen wie zum Beispiel DEIS, SECREDAS, BIECO (alle Horizon Europe), konnte eine fundierte Ausgangsbasis für das Projekt geschaffen werden.

0.5 Zusammenarbeit mit anderen Stellen

Innerhalb des Projekts war die FhG insbesondere aufgrund der leitenden Funktion im TP4, aber auch der Leitungsfunktion in verschiedenen Arbeitsgruppen (u.a. Core03) und der zentralen Einfindung in die Erarbeitung des Assurance Frameworks, mit praktisch allen Partnern direkt vernetzt und im wissenschaftlichen Austausch. Insbesondere ist zu nennen:

- Entwicklung der Phänomen-Signal-Analyse Methodik und der semantischen Normverhaltensanalyse mit Technischen Universität Braunschweig, ZF, Bosch und Prostep.
- Erarbeitung des Safety Assurance Frameworks und der darauf basierenden VVM Sicherheitsargumentation: IAV, TU Braunschweig – Institut für Regelungstechnik (IfR), Bosch, ZF.
- Ableiten von Gütekriterien mit Partner Bosch
- GQM-Methode mit Partner Ford
- Entwicklung der probFMEA/CFT Methodik zur systematischen Sicherheitsanalyse mit dem Fraunhofer LBF.
- Ableiten von System- und Testanforderungen mit Partnern Bosch, ZF, Conti
- Auswahl geeigneter Messstellen in Zusammenarbeit mit der Verkehrsunfallforschung an der TU Dresden GmbH (VUFO).
- Entwicklung einer XiL-Testumgebung mit dem FZI

1 Eingehende Darstellung

1.1 der Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

1.1.1 TP3

1.1.1.1 AP3.1 – Globale Sicherheitsbetrachtung

Im Arbeitspaket AP3.1 wurden wesentliche Ziele und gemeinsame Arbeitsschwerpunkte definiert, um die Grundlagen der Gefährdungsanalyse, der Phänomene, der Unfallstatistik und der Automationsrisiken mit besonderem Fokus auf Kreuzungssituationen zu erarbeiten. Die Gefährdungsanalyse und Risikoklassifizierung erfolgten nach ISO 2626-3, wobei die FhG seine Expertise auf dem Gebiet der funktionalen Sicherheit und Systemzuverlässigkeit einbrachte.

Phänomen-Signal-Modell (PSM)

Ein bedeutendes Ergebnis war die Entwicklung des Phänomen-Signal-Modells (PSM) und die semantische Analyse von Verhaltensnormen. Dies mündete in der Co-Autorschaft an den Publikationen „Phänomen-Signal-Modell: Formalismus, Graph und Anwendung“ sowie „Ein Beitrag zur semantischen Analyse und formalen Repräsentation von Verhaltensnormen für das automatisierte Fahren“. Zudem wurde ein Metamodell zur formalen Spezifizierung von PSM und semantischer Normanalyse erarbeitet und in die Digital Dependability Identity (DDI) integriert, um eine durchgängige Referenzierbarkeit zwischen Sicherheits- und Entwicklungsartefakten zu ermöglichen. Die Integration dieser Methoden in DDIs wurde demonstriert, indem ein DDI von FUC_2.3 erstellt wurde. Des Weiteren wurden Skripte programmiert, die einige Prozessschritte aus AP3.1 automatisierten, siehe Abb. 1.

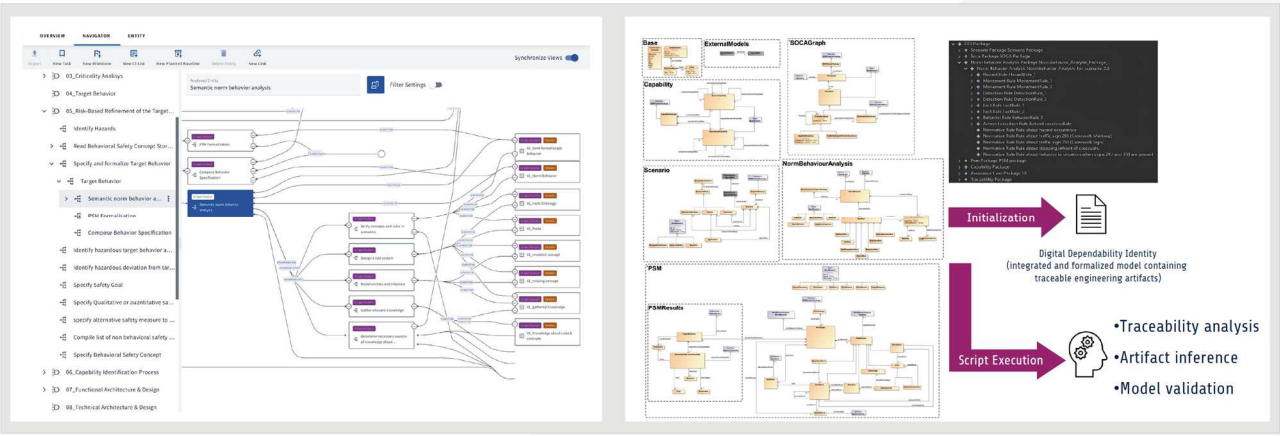


Abbildung 1: Inter-process und inter-artifact traceability mit TRACY (links) und DDI (rechts)

Ein Poster zum Halbzeitevent mit dem Titel „Digital Dependability Identities – A concept to manage complexity“ wurde erstellt und präsentiert. Hierbei wurde das Konzept der Digital Dependability Identities im Kontext von VVM vorgestellt, wobei die Vorteile der Formalisierung von VVM-Ergebnissen als Metamodelle erläutert und gezeigt wurden, wie verschiedene Ergebnisse aus der VVM-Methodik in einem DDI verknüpft sind. In der zweiten Projekhälfte wurde mit Prostep an der technischen Integration des DDI-Frameworks und dem Tracy-Tool gearbeitet. Die Arbeit ist im

Poster „Assuring Traceability of Development Processes and Artifacts in the Context of the VVM-Project“ des Final Events dokumentiert.

Abschließend verfasste das IESE einen Input zu Deliverable D02, der die Erzeugung formaler Traceability zwischen TP3-Konzepten mithilfe der ODE-Metamodellerweiterung beschreibt. Darin wird erläutert, wie der formale Metamodellansatz genutzt werden kann, um die in TP3 erarbeiteten Methoden und die daraus resultierenden Artefakte formal aus der Sicherheitsargumentation referenzierbar zu machen und diese Artefakte auch für konsumierende Methoden in modellbasierter Form verfügbar zu machen.

Das LBF brachte einen essenziellen Beitrag zur Entstehung des methodischen Ansatzes zur Abbildung und Analyse von kognitiven Zusammenhängen zwischen Verkehrsteilnehmern, automatisierten Fahrzeugen und der Umgebung im Kontext des Verkehrsgeschehens. Der Beitrag des LBF beruhte auf der initialen Schaffung eines Notationsschemas und zugehöriger Symbolik. Dieser beruht auf der seitens Bosch vorbereiteten Phänomenalgebra und erlaubt deren ideellen Bestandteile in einem intuitiv erfassbaren Notationsschema im Zusammenhang modellhaft abzubilden, sodass das Modellabbild eine Beschreibung von Abläufen und darin entstehende Wahrnehmungs- und Verhaltensprozesse gemäß deren logisch-kausalen Zusammenhangs wiederzugeben. Das initial vom LBF erarbeitete Konzept wurde in einer bilateralen Telefonbesprechung zwischen Bosch und LBF diskutiert und in Details optimiert, mit dem in den Abbildungen 2, 3 und 4 zur Signalanalyse dargestellten Zwischenergebnis. Dieses unterliegt aktuell der weiteren Prüfung, Ausarbeitung und Interpretation anhand weiterer Beispielszenarien. Zudem wird in der Folgezeit eingehender untersucht, welche qualifizierten Aussagen möglicherweise über den Zweck der ausschließlichen Notation hinaus mit den Modellen generiert werden können. Ferner sind Aktivitäten geplant, das bestehen inhaltlicher Zusammenhänge mit anderen Methoden und Verfahren zu ermitteln und Möglichkeiten eines synergetischen Anwendungskonzepts der betreffenden Techniken auszuarbeiten.

Objekt / Effekt (was ist / Ergebnis)	**Index**	**Symbol**	**Bedeutung**
Ereignis, Geschehnis	P_{ξ}		Emanation
Signale, Geschehnis	P_{π}		Perzeption / empfangene Information
Handelnde, Aktion	αA		Aktion
Handelnde, Erwartung	αE		Antizipation
Umgebung, Geschehnis	P_{Ω}		Phänomen
Umgebung, Information	ΩW		immanente Information
Signal, Information	πW		emittierte Information (i.S.v. „perceive“)

Abbildung 2: Notationsschema und zugehörige Symbolik

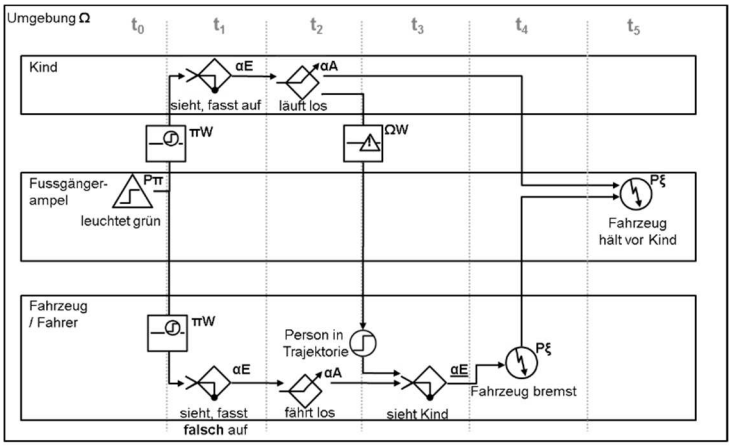


Abbildung 3: Beispielszenario Fahrer sieht Kind und bremst infolgedessen

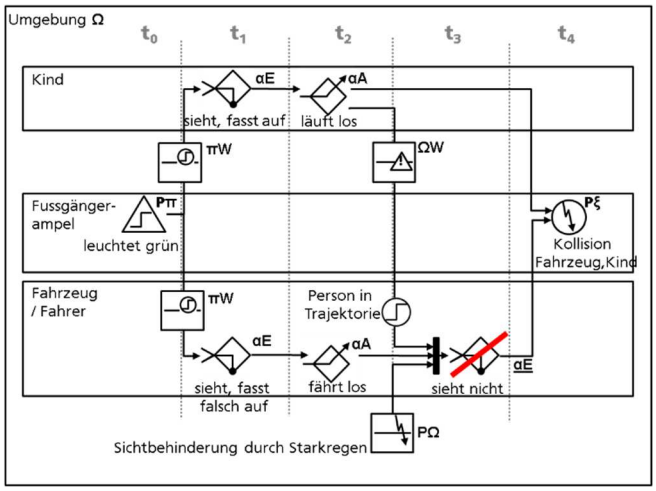


Abbildung 4: Beispielszenario Fahrer kann Kind nicht sehen, Kollision ereignet sich

Auf Basis dieser Darstellungsweise wurden in regelmäßigen Arbeitstreffen im PSM-Kernteam zusammen mit Bosch, ProStep und Fraunhofer IESE diverse Fragen zu inhaltlichem Aufbau, Möglichkeiten der Auswertung und Verknüpfung mit übergeordneten Fragestellungen und Sicherheitsnachweisstrategien, sowie Umsetzbarkeit einer PSM-Simulationssoftware (federführend Bosch) behandelt. Unter anderem beteiligte sich LBF an dem Aufbau eines Metamodells zur SysML-Modellierung von PSM-Darstellungen unter Federführung von IESE. In Zusammenarbeit mit ProStep bereitete LBF dazu eine erste PSM-Darstellung des durchgängigen Beispielszenarios „Annäherung an einen Fußgängerüberweg“ vor (siehe Abbildung 5). Anhand dieses Beispiels wurde die Instanziierung eines SysML-Modells aus dem Metamodell in Zusammenarbeit von IESE, ProStep, Bosch und LBF vorgenommen.

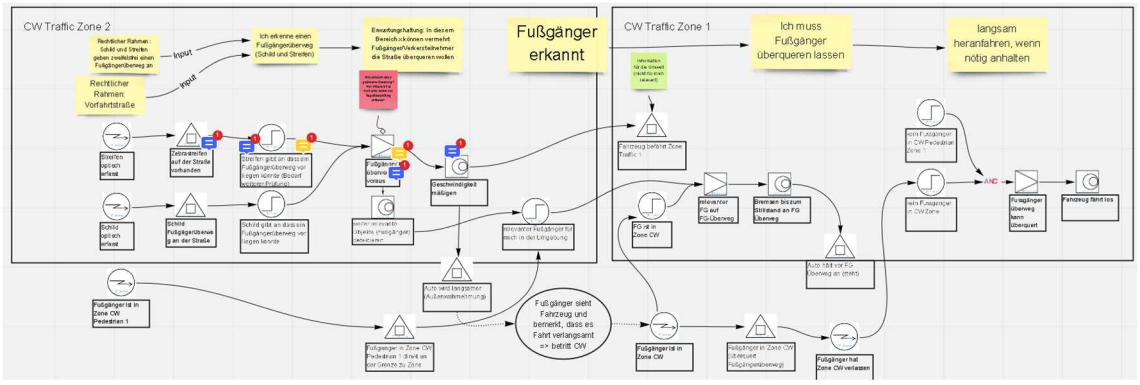


Abbildung 5: Arbeitszwischenstand des PSM zum Szenario „Annäherung an einen Fußgängerüberweg“ von ProStep und LBF als vorbereitender Beitrag zur Erarbeitung des PSM-Metamodells von IESE

1.1.1.2 AP3.2 – Lokale Sicherheitsbetrachtung

Im Arbeitspaket AP3.2 konzentrierte sich die FhG auf die methodische Spezifikation und Verifikation von Sicherheitsanforderungen, die auf einer Analyse der funktionalen Sicherheit und Systemzuverlässigkeit basierten. Wesentliche Beiträge umfassten die Erarbeitung von Methoden der funktionalen Sicherheit und des Risikomanagements. Die Systematik zur Ableitung von Metriken zur Messung von Risiken und die Verwendung von risikominimierenden Maßnahmen und Fahrmanövern wurden ebenfalls vom IESE mitentwickelt.

Eine bedeutende Veröffentlichung in diesem Zusammenhang war die Journal-Publikation zum Risk Management Core, die in 2024 veröffentlicht wurde. Hierbei wurde insbesondere die Verbindung zwischen dem Risk Management Core und der projektübergreifenden Sicherheitsargumentation aus der Core03-Gruppe integriert.

Zudem wurden im Rahmen von AP3.2 erste Teile einer systematischen Methode entwickelt, um die ODD (Operational Design Domain) Beschreibung für bestimmte Safety Engineering Prozesse zu verbessern. Diese Ergebnisse wurden auf dem Final Event in Form des Posters „Guideword-based ODD tailoring: Towards making ODD descriptions processable for different stakeholder“ präsentiert. Diese Arbeiten tragen dazu bei, die Sicherheit und Zuverlässigkeit der entwickelten Systeme durch eine verbesserte Prozessierbarkeit der ODD-Beschreibungen für verschiedene Stakeholder zu gewährleisten.

Aufgrund der Priorität, einen projektübergreifenden Sicherheitsnachweis zu erzeugen (Begründung siehe Kapitel 0.3), wurden die ursprünglich vorgesehenen Aufgaben zur dynamischen Risikobewertung in AP3.2 zugunsten der Arbeiten in Core03 verlagert.

1.1.1.3 AP3.3 – Sicherstellung Durchgängigkeit Argumentationsstruktur

Im Arbeitspaket AP3.3 fokussierte sich die FhG auf die Modellierung der Argumentationsstruktur mittels der Goal Structuring Notation (GSN) und die generische Integration von funktionalen Sicherheitskonzepten in die Argumentationsstruktur. Ein zentraler Aspekt war der Aufbau einer Sicherheitsargumentation bezüglich des dynamischen Risikomanagements und deren Integration in den übergeordneten lokalen und globalen Sicherheitsnachweis.

Aufgrund der wenigen vorgesehenen FhG-Projektaufwände in AP3.3 (3PM über gesamte Projektlaufzeit) wurde Core03 zur Erzeugung der projektübergreifenden Sicherheitsargumentation in TP4 aufgehängt und die Beiträge des IESE in A3.3 beschränkten sich auf die projekt-interne Kommunikation, sodass die Kompatibilität der Sicherheitsargumentation für den Risk Management Core mit der projektübergreifenden Sicherheitsargumentation sichergestellt wurde.

Dazu organisierte das IESE einen Workshop in Braunschweig in 2023, der darauf abzielte, den Risk Management Core in die Gesamtargumentation zu integrieren. Dieser Workshop förderte die Zusammenarbeit und stellte sicher, dass die AP3.3-spezifischen Methoden und die Sicherheitsargumentation nahtlos in die projektübergreifende Struktur eingebettet sind. Dies trägt wesentlich dazu bei, die Einheitlichkeit und Durchgängigkeit der Sicherheitsnachweise im gesamten Projekt zu gewährleisten.

1.1.1.4 AP3.4 – Ableitung einer exemplarischen funktionalen Systemarchitektur

Das LBF beteiligte sich an der Klärung der Ermittlung und Darstellung der der Systemarchitektur, sowie der Herangehensweise zur Erstellung der diesbezüglichen Arbeitsergebnisse. Die Architektur stellt einen wesentlichen Informationsträger zur Erfassung und Überführung konzeptioneller Anforderungen und Spezifikationen (aus TP3) in die funktionale Implementierung der Systemkomponenten und –funktion (TP4) dar. Zudem stellt sie grundsätzlich ein essenzielles Element dar, um Sicherheitsanforderungen auf Fahrzeugebene in dedizierte Sicherheitsanforderungen und –spezifikationen innerhalb der Fahrzeugbestandteile ausdifferenzieren zu können. Im Kontext des automatisierten Fahrens bestehen neben der grundsätzlichen Herausforderung, den damit verbundenen wesentlich erweiterten Raum des zu beschreibenden Systemverhaltens vollständig zu erfassen und darstellen zu können, die grundsätzlich neue Qualität des eigenverantwortlichen Entscheidens und Handeln des virtuellen Fahrers. Hierfür besteht keine allgemein erwiesene oder anerkannte methodische Technik für deren Erfassung und Beschreibung bzw. ist diese prinzipiell noch nicht verfügbar.

LBF verfolgte in diesem Kontext die Erfüllung der aktiven Gestaltung der Rolle als Schnittstellenfunktion zwischen den betreffenden TP3 und 4. Hierzu wurde im Rahmen der TP3 Regel-Telefonkonferenzen ein Impulsvortrag gehalten mit dem Ziel, hervorgegangene Diskussionen und Abstimmungen zu einer gemeinsamen Sichtweise zu fokussieren. Dies erfolgte in wunschgemäßem Ausmaß, sodass sich ein grundsätzlicher Konsens über die zu behandelnden Inhalte und deren Auffassung festhalten ließ. Zudem ergab sich die Maßnahme, die Thematik weiter im Zuge der nun zu initiierenden TP3.4 Regelbesprechungen zu behandeln.

Weiter war das LBF in der regelmäßigen TP3.4-Arbeitsgruppe aktiv und gestaltete die Diskussionen und Klärungen weiterhin aktiv mit. Inhaltlich erfolgte dies im Rahmen der diesbezüglichen Darstellungen, die an dieser Stelle in den vorigen Berichtszeiträumen ausgeführt wurden. Daher sei hiermit auf diese verwiesen. Als Besonderheit sei die intensive Vorbereitungsphase gemeinsam mit den Team-Partnern auf das Halbzeitevent erwähnt.

Besonderen Aufwand investierte LBF zudem in die Querschnittsarbeit mit der TP4-Gruppierung zur Fehleranalyse mit probFMEA/CFT. So nahm das LBF in der Rolle als TP3-Vertreter an den regelmäßigen Arbeitsterminen des Kernteams teil, um die TP3-Systematiken in den Ansatz der systemorientierten Verhaltens- und Technikfehleranalyse einzubringen und hier eine durchgängige Anbindung zu ermöglichen. Das betrifft sowohl die Systematik der Fähigkeitenarchitektur aus TP3.4,

als auch des PSM-Ansatzes im TP3.1. Dies erfolgte im 1. Halbjahr 2022 zu einem Großteil in Form der maßgeblichen Mitgestaltung der Vorbereitungen, Abstimmungsrunden und der Durchführung der Präsentation im HZE (siehe Abbildung 6). Weitere Einzelheiten hierzu werden im Berichtsteil des TP4 geliefert.

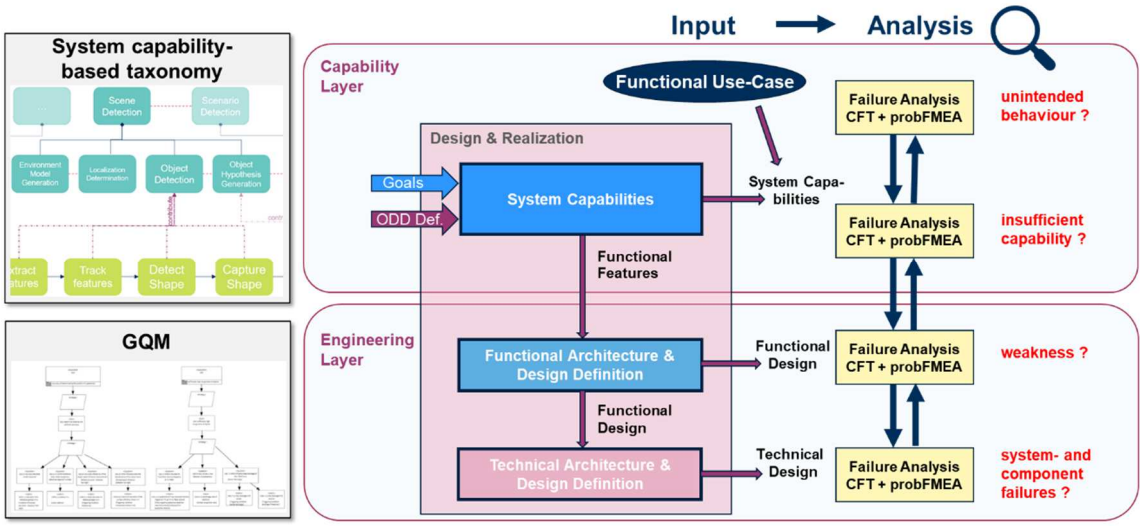


Abbildung 6: Zusammenhang zwischen der Methodik zur Fehleranalyse mit anderen methodischen Ansätzen im Zusammenspiel mit der fähigkeitsbasierten Systemtaxonomie (TP3) und GQM (TP4) als TP-übergreifendes Konzept.

1.1.2 TP4

1.1.2.1 AP4.1 – Methodik zur Ableitung von System- und Testanforderungen

Das übergeordnete Ziel von AP4.1 ist es, Methoden zu entwickeln, wie aus der funktionalen Systemarchitektur und dem notwendigen Sicherheitskonzept nicht-wettbewerbsdifferenzierende System- und Testanforderungen bestimmt werden können. Nachdem im Zuge von Ergebnis E4.1a erste grobe Gütekriterien erarbeitet wurden, soll in AP4.1 im Anschluss ein konzeptionelles Gerüst der Methodik entworfen werden, um System- und Testanforderungen abzuleiten.

Kritikalitätsmaß und Gütekriterien

LBF brachte sich in die Durchführung der Arbeiten der Arbeitsgruppe 4.3 „AG3 – Kritikalitätsmaß und Gütekriterien“ ein. Dies gestaltete sich in Form der aktiven Teilnahme an den regelmäßigen Arbeitssitzungen und dabei geleisteter Diskussionsbeiträge, sowie gelegentlich zusätzlicher Vor- und Nachbetrachtung der erarbeiteten Inhalte.

Besonders hervorzuheben ist die federführende Erarbeitung eines Auffassungskonzepts zu den Themen Güte, Gütekriterien und Kritikalitätsbegriff. LBF stand hierbei in bilateraler Abstimmung mit Bosch hinsichtlich sinnfälliger Strukturierungsansätze und inhaltlicher Eckpunkte und übernahm im Anschluss die Umsetzung und Präsentation in der AG-Runde (siehe Abbildung 7: Ideeller schematischer Zusammenhang zwischen den Begriffen Güte, Kritikalität und Wirkstruktur). Wesentliche Erkenntnisinhalte hierbei waren insbesondere die Sichtweise, dass sich Zwecke und Zielsetzungen auf eine jeweilige Ebene beziehen, wie beispielsweise die Welt-, Fahrzeug- oder Bauteilebene, wobei sich die Zielsetzungen untergeordneter Ebenen auf Zielsetzungen und Zwecke der übergeordneten Ebenen beziehen, d.h. zu diesen beitragen. Somit zeichnet sich ab, dass sich

für Ziele auf jeder der Ebenen zugehörige Gütekriterien definieren lassen, anhand derer der Grad der Zweckerfüllung bemessen werden kann bzw. das nicht Unterschreiten eines festzulegenden erforderlichen Mindestmaßes hinsichtlich der ausreichenden Güte. Unterhalb dieses Mindestmaßes liegt eine unzureichende Güte vor. In diesem unzureichenden Bereich wiederum befindet sich ggf. als Untermenge der Bereich, in dem die ungenügende Zweckerfüllung eine Kritikalität birgt. Dies gilt für solche unzulänglichen Eigenschaftsausprägungen, die ein potenziell kritisches Verhalten im Betrieb aufwerfen würden. Diese Begriffsauffassung kann dabei nur unter der Implikation gelten, dass ein als mit hinreichender Güte vollzogenes ideales Verhalten per Definition unkritisch ist.

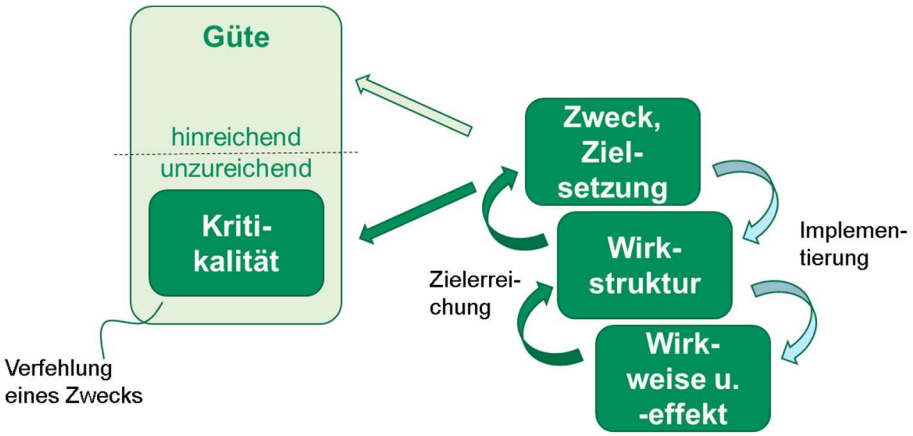


Abbildung 7: Ideeller schematischer Zusammenhang zwischen den Begriffen Güte, Kritikalität und Wirkstruktur

Weiter war der Erkenntnisbeitrag hier von Bedeutung, dass die Kritikalität im Zuge der Perspektiven der verschiedenen Ebenen des Welt- und Systemmodells jeweils spezifische Abgrenzungen und damit verbundene Kontexte hat. Da sich eine Reihe der VVM-Teilprojekte anhand derer Betrachtungsschwerpunkte jeweils betreffenden Ebenen zuordnen lassen, kann auch der dort behandelte Kritikalitätsbegriff (vorschlagsweise) bestimmten thematischen Zusammenhängen und thematischer Umfänge zugeordnet werden:

Kritikalität im

- TP2: Kontext der Verkehrsmechanik mit generischem Fahrzeug
- TP3: im Sinne von (gefährlicher oder allgemeiner) Verletzung von Normverhalten
- TP4: im technischen Sinne
    - gefährdungsfrei valide Performance („SOTIF“; Brücke zu TP3)
    - Traditionelle Functional Safety (ISO 26262)
        - Güte der technischen Implementierung, Absicherung (ASIL), Roadworthiness
        - Bezugsrahmen ist Fahrzeug, das schon fahren kann
- TP7: Kritikalität in Bezug auf Erfüllung der Testkriterien und Testbarkeit (Möglichkeit / Annahme)

Probabilistische FMEA mit Component Fault Trees (probFMEA/CFT)

Als wesentlichen Arbeitsinhalt des TP4 konzentrierte sich Fraunhofer auf die Entwicklung und Erweiterung von Safety-Analyse-Methoden zur Untersuchung der Sicherheit von autonomen Fahrzeugen. Gemeinsam mit dem Fraunhofer LBF wurden Methoden entwickelt, die auf der probabilistischen FMEA und der Component Fault Tree (CFT) Analyse basieren, um System- und Testanforderungen abzuleiten, siehe Abb. 8. Dabei wurden funktionale Use-Cases, das Soll-Verhalten und Sicherheitsziele als Input vorausgesetzt. Der Ansatz ermöglichte die Analyse auf verschiedenen Abstraktionsebenen, darunter die Fähigkeiten, die funktionale Architektur und die technische Architektur des Fahrzeugs.

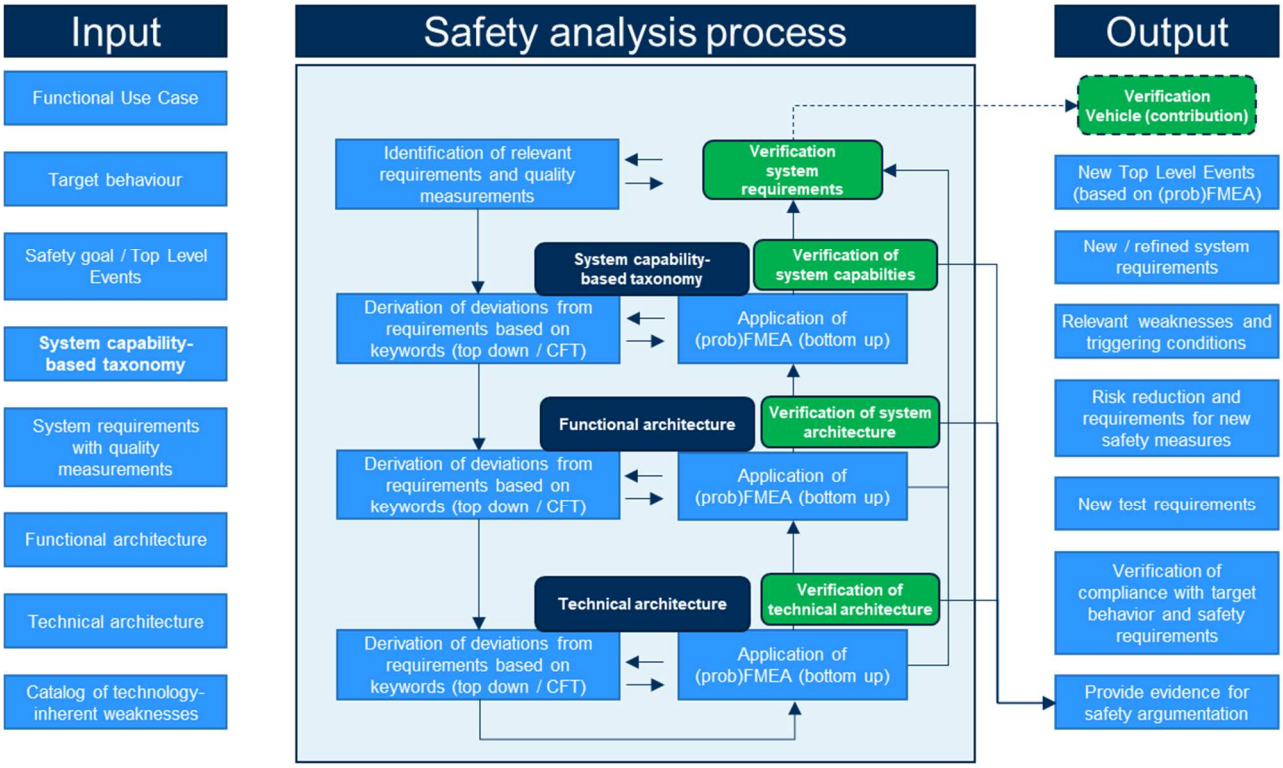


Abbildung 8: Überblick probFMEA/CFT Methodik

Eine zentrale Aufgabe bestand in der Erweiterung der CFT-Analyse, indem neben den klassischen Systemfehlern auch Sensorschwächen und mögliche Triggerbedingungen berücksichtigt wurden. Dies ermöglichte die Identifikation von Ursachen für Sicherheitszielverletzungen und die Beurteilung, ob die implementierten Sicherheitsmaßnahmen die Risiken ausreichend minimieren. Ergänzend dazu wurde die probFMEA Methodik als Bottom-up-Analyse eingesetzt, um die Wahrscheinlichkeiten gleichzeitig auftretender Effekte und deren Folgen zu analysieren.

Diese Analysen wurden zur Ableitung neuer Anforderungen, zur Identifikation geeigneter Sicherheitsmechanismen und zur Erstellung geeigneter Testfälle während der Entwicklung verwendet. Zudem verifizierte die Analyse die Sicherheit der Architektur für die gegebenen Einsatzszenarien als Teil der Sicherheitsargumentation. Die Konzepte wurden im Tool SafeTbox umgesetzt, das die Modellierung von Architekturen und Safety-Konzepten verbindet. Das Tool ermöglicht die Bestimmung und Bewertung kritischer Kombinationen von Events durch eine integrierte Minimal-Cut-Set Analyse.

Die Ergebnisse und Methoden wurden im Rahmen der Fachtagung „Technische Zuverlässigkeit“ 2021 publiziert und präsentiert (Rauschenbach, M., Kupjetz, S. M., Wolschke, C., & Braun, T. (2021). Ansatz zur methodischen Analyse und Absicherung des Funktionalkonzepts voll automatisierter Kraftfahrzeuge). Auf dem Halbzeitevent wurde ein Vortrag und ein Poster erstellt, die die methodischen Ansätze und die praktische Anwendung der entwickelten Methoden detailliert beschrieben und demonstrierten. Zusätzlich wurden auf dem Final Event ein Demonstrator sowie zwei Poster mit den Titeln „safeTbox: Tooling for Safety Analysis“ und „Safety Analysis of (In-)Capabilities and Weaknesses using Component Fault Trees and probFMEA“ vorgestellt. Diese Arbeiten trugen dazu bei, die Konsistenz und Nachverfolgbarkeit der Sicherheitsnachweise im gesamten Projekt zu verbessern und eine formale Verbindung zwischen den entwickelten Methoden und den Sicherheitsanforderungen herzustellen.

Zur Erarbeitung eines Gerüsts der Methodik, wurden die Erkenntnisse aus dem PEGASUS-Bericht zur Identifikation und Quantifizierung von Automationsrisiken für hochautomatisierte Fahrfunktionen aufgegriffen[1], Abb. 9.

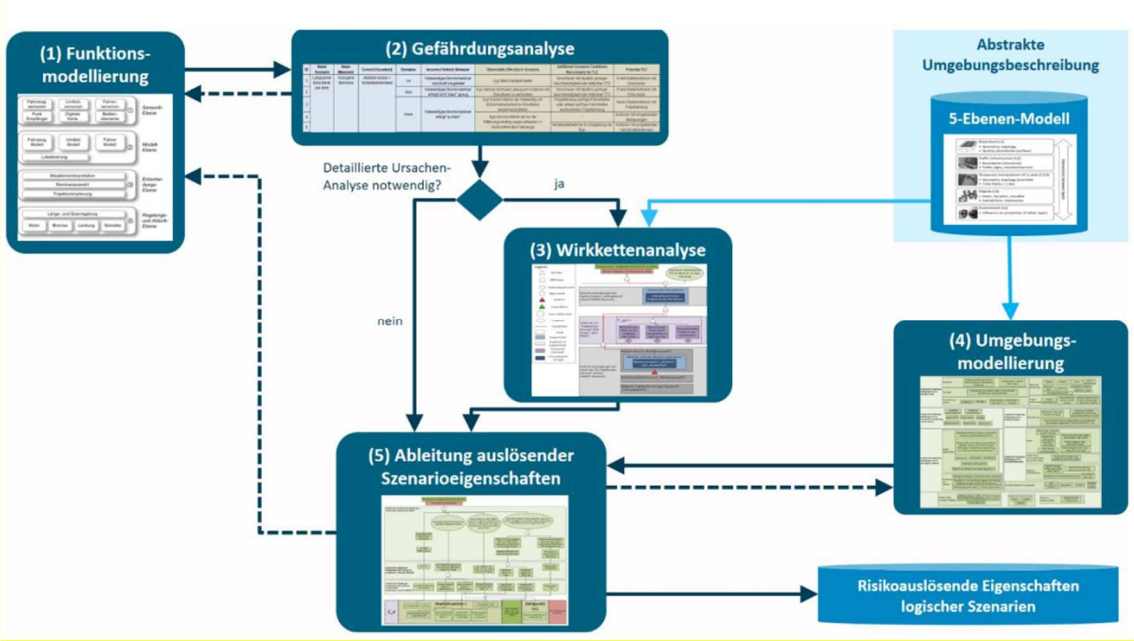


Abbildung 9: Methode zur Identifikation von Automationsrisiken aus Pegasus[1]

In diesem Bericht wird eine selbstentwickelte Methode beschrieben, mit der Automationsrisiken identifiziert werden können. Dies basiert auf existierenden Methoden der Gefahren- und Risikoanalyse und wurde für SAE-Level 3 und höher angepasst. Die entwickelte Methodik wurde im Rahmen der Publikation „Ansatz zur methodischen Analyse und Absicherung des Funktionalkonzepts voll automatisierter Kraftfahrzeuge[2]“ beschrieben und detailliert dargestellt. Die entwickelte Methode wurde auf die hochautomatisierten Fahrfunktion (HAF) Autobahn-

[1] Eckard Böde; Matthias Büker; Werner Damm; Martin Fränzle; Birte Kramer; Christian Neurohr; Sebastian Vander Maelen (2019): Identifikation und Quantifizierung von Automationsrisiken für hochautomatisierte Fahrfunktionen. Online verfügbar unter https://www.pegasusprojekt.de/files/tmpl/pdf/PEGASUS_TechnicalReport_Automationsrisiken_17.07.2019.pdf .

[2] M. Rauschenbach, C. Wolschke, T. Braun, S. Kupjetz; Technische Zuverlässigkeit 2021. Entwicklung und Betrieb zuverlässiger Produkte: 30. VDI-Fachtagung; Online-Tagung, 27.-28.04.2021

Chauffeur angewandt. Die allgemeine Methode zur Identifikation von Automationsrisiken ist in Abbildung 9 dargestellt. Als erster Schritt werden die Funktionen modelliert (1) und anschließend wird eine Gefährdungsanalyse durchgeführt (2). Wenn eine detaillierte Ursachenanalyse notwendig ist, erfolgt eine Wirkkettenanalyse (3). Als Input für die Wirkkettenanalyse und die Umgebungsmodellierung (4) dient eine abstrakte Umgebungsbeschreibung (5-Ebenen-Modell). Aus (2), (3), (4) lassen sich auslösende Szenarioeigenschaften ableiten (5), die später als risikoauslösende Eigenschaften logischer Szenarien gesammelt werden können. In PEGASUS wurde die hochautomatisierte Fahrfunktion *Autobahnchauffeur* auf mögliche auftretende Automationsrisiken untersucht und eine quantitative Auswertung szenariobezogener Schwächen vorgenommen. In VVMethoden erhöht sich die Komplexität des betrachteten Systems durch das Vorliegen einer vollautomatisierten Fahrfunktion. Die Randbedingungen lassen sich aus diesem Grund nicht vollständig determinieren. Das Fahrzeug generiert das Verhalten durch den hohen Automationsgrad selbständig – die Rückfallebene zur Bewältigung kritischer Situationen/Problemen durch die Übergabe der Kontrolle an den Fahrer entfällt.

Gebräuchliche Methodensysteme zur Fehleranalyse im Bereich der Funktionalen Sicherheit sind in der ISO 26262 zu finden. Zum einen beinhaltet diese die Gefährdungsidentifikation und Risikoklassifizierung (HARA) und zum anderen System- und Komponentenfehleranalysen mit FMEA und FTA. Zur Identifikation und Beherrschung von Schwächen funktionaler Komponenten existiert die Norm ISO 21448 (safety of intended functionality – SOTIF). Zwischen möglichen Gefahren und gefährlicher Funktionalabweichung besteht eine methodische Lücke. Die funktionale Reaktion lässt sich a priori nicht spezifizieren, sondern wird anhand eigener Einschätzung durch das System erzeugt. Es besteht daher eine Lücke im methodologischen Konstrukt zur Spezifikationsanalyse. Um in der vorherrschenden Situation eine angemessene und sichere funktionale Antwort hervorbringen zu können, ist eine erforderliche Fähigkeit, die sichergestellt werden muss. Die Verifikation kann anhand erforderlicher Fähigkeiten erfolgen, um in allen Situationen sicher reagieren zu können.

Zur Fehleranalyse werden Component Fault Trees (CFT) und die probabilistische FMEA (probFMEA) eingesetzt. Ziel der Kooperation zwischen LBF und IESE ist es dabei die beiden methodisch etablierten Ansätze und deren Stärke systematisch zu einer Methodik zu verbinden. Am Fraunhofer IESE wird die Methodik der CFT in wissenschaftlichen und industriellen Projekten eingesetzt und weiterentwickelt. Mit diesem Ansatz wird ein modularer, hierarchischer Top-Down-Ansatz verfolgt, der eine Modellierung der Fehlerpropagation ermöglicht. Zur effizienten Anwendung kommt das eigens entwickelte Tool SafeTBox[3] zum Einsatz, welches als Plugin in das SysML/UML-Modellierungprogramm Enterprise Architect[4] integriert wurde.

[3] Webseite der SafeTBox vom Fraunhofer IESE: https://www.safetbox.de/
[4] Webseite von Enterprise Architect: https://www.sparxsystems.com/products/ea/index.html

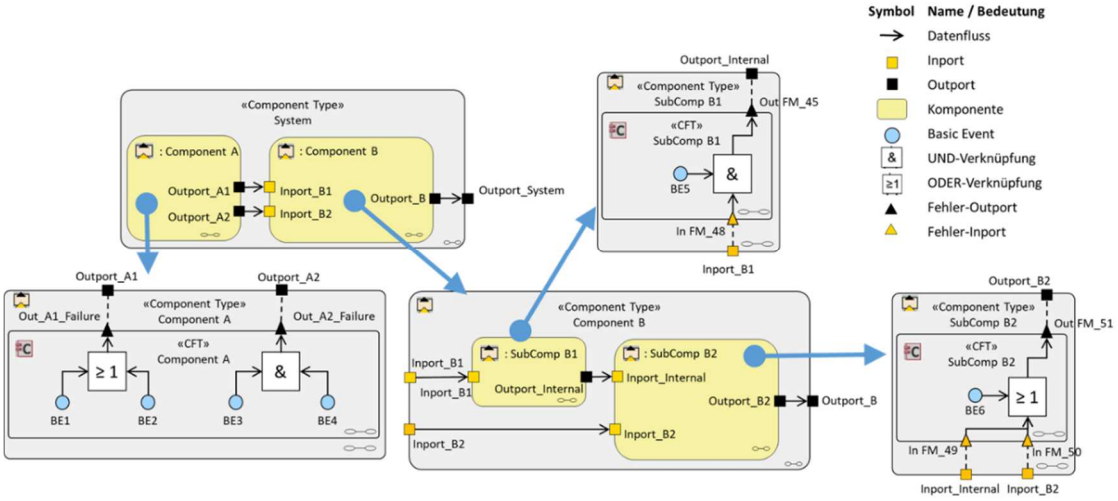


Abbildung 10: Beispielhafte CFT mit Legende

In Abbildung 10 ist ein beispielhafter Ausschnitt eines CFT abgebildet, welcher die Fehlerpropagierung zwischen Komponenten beschreibt. Der Zusammenhang zur Systemarchitektur und den dort als Funktionsnetz modellierten Datenflüssen erfolgt über die In- und Out-Ports, der Komponenten und der mit den Ports verbunden Fehler-Out-Ports und Fehler-In-Ports der Fehlermodelle (vgl. Component A). Die Ursachen von Fehlern werden mittels Basic Events modelliert. Für eine logische Verknüpfung der Ereignisse stehen UND- und ODER-Verknüpfungen zur Verfügung.

Durch die direkte Verknüpfung der gezeigten Fehlermodelle mit den funktionalen Komponenten der Architektur (funktionale Komponenten oder Fähigkeiten innerhalb der Fähigkeiten basierten Architektur) ist zu jedem Zeitpunkt innerhalb der Entwicklung die Nachverfolgbarkeit und Konsistenz gewährleistet: Das Fehlermodell und fehlerhafte Verhalten lässt sich direkt den Komponenten der Architektur sowie den Schnittstellen zuordnen, die bzgl. der Interaktion involviert sind.

Bei der Top-Down-Analyse wird beginnend von der Verletzung eines Sicherheitsziels bzw. einer Sicherheitsanforderung die Fehlerpropagierung entlang des modellierten Datenflusses und den Komponentenschnittstellen modelliert, bis hin zur Fehlerursache innerhalb der Komponenten. Die Ursachen werden durch die Basic Events (BE) innerhalb des Fehlermodells repräsentiert. Die methodischen Details zu CFT finden sich in [5] und [6]. Die anschließende Analyse der Minimal-Cut-Sets zeigt, welche Maßnahmen bei welchen Bedingungen aktiv sind und ermöglichen dem Safety Engineering zu beurteilen, ob die Maßnahmen hinreichend sind, um das resultierende Risiko auf ein akzeptables Maß zu reduzieren.

Der klassische Ansatz bzgl. Fehlerbäumen berücksichtigt jedoch ausschließlich Aspekte funktionaler Sicherheit. Im Rahmen der Arbeit in TP4 wurde untersucht, welche Erweiterungen für die Berücksichtigung der SOTIF-Fragestellungen im Kontext hochautomatisierter Fahrfunktionen und die Berücksichtigung relevanter Umgebungsbedingungen und –situationen erforderlich sind (siehe unten). Abbildung 11 zeigt im unteren Zweig die Kombination von CFT (Top-Down-Ansatz) und probFMEA (Bottom-Up-Ansatz) sowie im oberen Teil die Schnittstellen zu den anderen

[5] Kaiser, B., Liggesmeyer, P., Mäckel, O.: A new component concept for fault trees. In: Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software, pp. 37–46 (2003)
[6] Kaiser, B., Schneider, D., Adler, R., Domis, D., Möhrle, F., Berres, A., Zeller, M., Höfig, K., Rothfelder, M.: Advances in component fault trees. In: Proceedings of ESREL (2018)

Arbeitspaketen, welche für die Berücksichtigung von SOTIF-Aspekten mit ihren Vorarbeiten und deren Input innerhalb des Projektes für die Ausarbeitung der Methodik erforderlich sind.

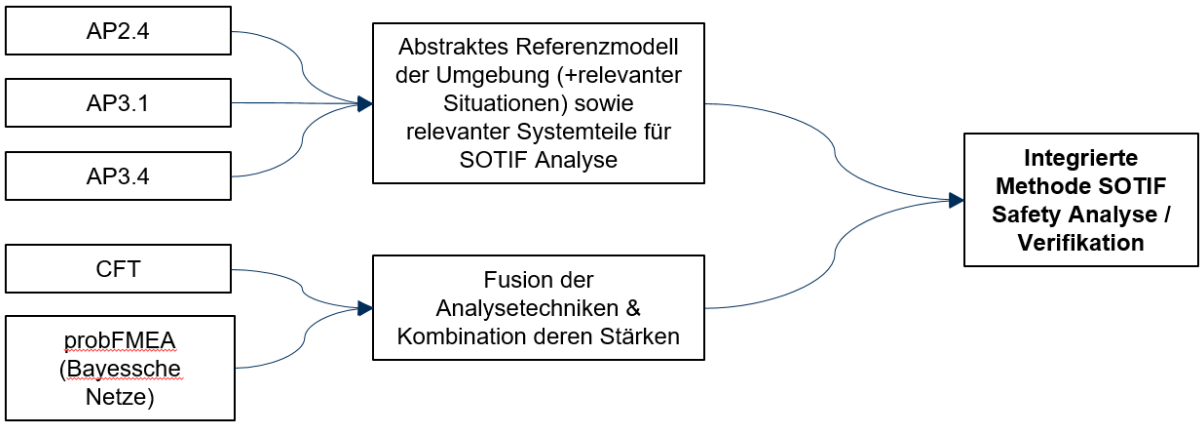


Abbildung 11: Vorgehen zur integrierten Methode SOTIF Safety Analyse / Verifikation

Zur Bottom-Up-Analyse der Fehler wird ergänzend zur CFT die probabilistische FMEA (probFMEA) eingesetzt. Hiermit lässt sich ein logisches Netzwerk der Kausalbeziehungen (Ursache-Folge) erzeugen. Die Modellierung und Berechnung der Folgewahrscheinlichkeiten erfolgt in Bayesschen Netzwerken.

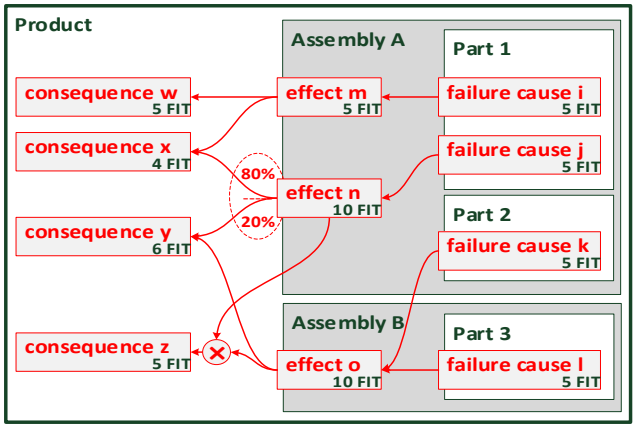


Abbildung 12: Schema der probabilistischen FMEA (probFMEA)

In Abbildung 12 ist schematisch dargestellt, wie eine probabilistische FMEA aufgebaut ist. Hierbei führt eine Fehlerursache innerhalb einer Komponente, die eine gewisse Ausfallwahrscheinlich besitzt (z. B. 5 FIT – 5 Ausfälle je 10^9 h) zu einem Effekt auf der Ebene der Baugruppe mit einer Folgewahrscheinlichkeit. Die Auswirkungen verschiedener Fehlereffekte und dessen Konsequenzen auf Produktebene lassen sich ebenfalls mit den entsprechenden Wahrscheinlichkeiten darstellen.

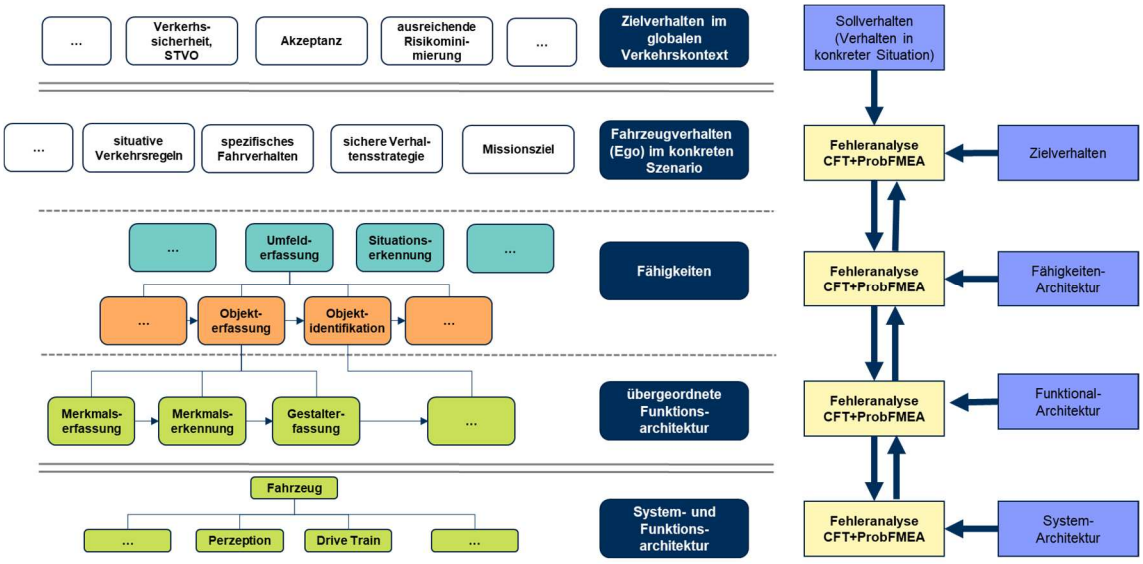


Abbildung 13: Analyse der Fähigkeitenarchitektur

Aufbauend auf Nolte et al.[7] ist eine Analyse der Fähigkeitenarchitektur Teil des Ansatzes, wobei sich die entwickelte Methodik wie in Abb. 13 dargestellt auf verschiedenen Abstraktionsebenen nutzbringend anwenden und diese im Sinne einer Verfeinerung/Abstraktion miteinander verbindet. Die grundlegende Methodik ist hierbei identisch für die unterschiedlichen Abstraktionsebenen, jedoch unterscheidet sich Gegenstand und Fragestellung bei der Analyse: Von dem Fahrzeugverhalten in einem konkreten Szenario über die System-/Fähigkeitenarchitektur bis zur Funktions- und technischen Architektur (letztere ist in dem Diagramm nicht dargestellt, da diese den Anspruch hinsichtlich *nicht wettbewerbsdifferenzierend* nicht zwingend erfüllt). Auf dem obersten Level des Zielverhaltens im globalen Verkehrskontext steht das Sollverhalten, welches sich auf das Verhalten in einer konkreten Situation bezieht. Unter diesem Level befindet sich das Verhalten des Egofahrzeugs in einem konkreten Szenario. Weiter unten befinden sich die Fähigkeiten, die übergeordnete Funktionsarchitektur und die System- und Funktionsarchitektur. Als Input für die Analyse wird dazu das Soll- und Zielverhalten, die Fähigkeiten-, Funktional und Systemarchitektur genutzt (je nach Abstraktionslevel). Ziel ist es, auf Basis der Modellierung der Fehlermodelle und anschließenden Analysen (Minimal-Cut-Set, Bayessche Netze) geeignete Maßnahmen abzuleiten und diese im Rahmen der jeweiligen Architekturen z.B. als zusätzliche Fähigkeiten oder Funktionen einfließen zu lassen. Abschließend kann durch eine erneute Analyse der modifizierten Architektur ein Beleg für die Risikoreduktion und somit der Effektivität der Maßnahmen erbracht und in die Sicherheitsargumentation als Evidenz einfließen gelassen werden.

[7] Nolte, M. et al.: „Towards a Skill- and Ability-Based Development Process for Self-Aware Automated Road Vehicles“, ITSC (IEEE), 2017.

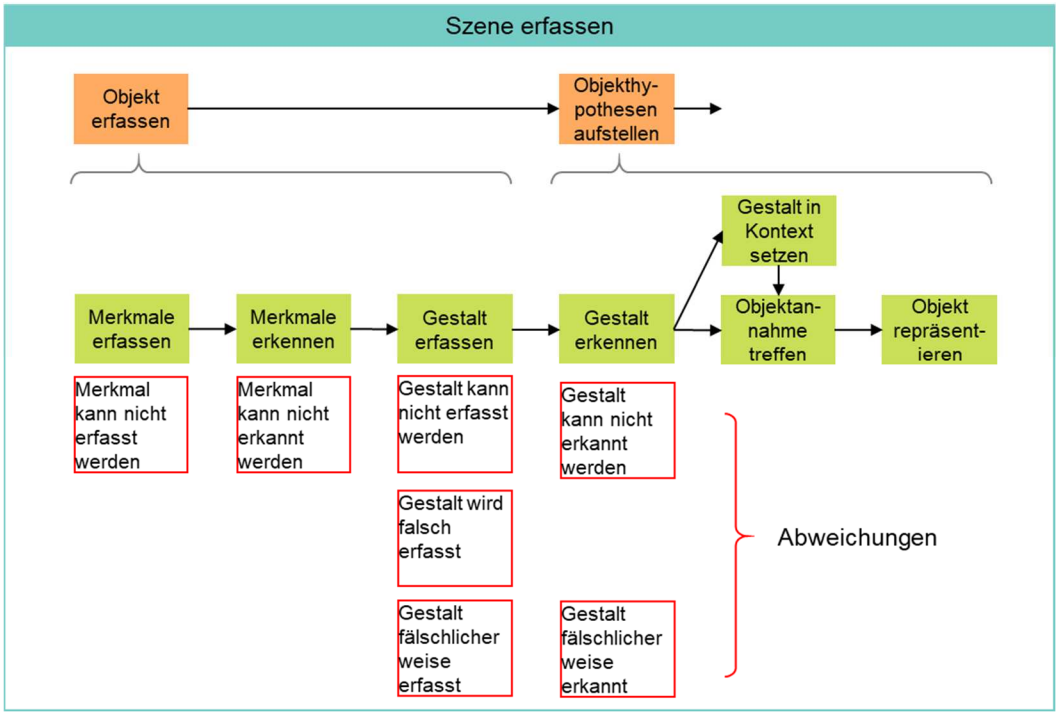


Abbildung 14: Analytische Ermittlung der Fehlerursachen von Fähigkeitsbeeinträchtigungen und –defiziten

In Abbildung 14 ist dargestellt, wie die Fehlerursachen von Fähigkeitsbeeinträchtigungen und –defiziten für die Fähigkeit „Szene erfassen“ analytisch ermittelt werden sollen. Teil von „Szene erfassen“ sind die Unterfähigkeiten „Objekt erfassen“ und „Objekthypothesen aufstellen“. Für die systematische Identifikation der Fehler kann hierbei die HAZOP-Methodik angewendet werden, welche stark in der FMEA-Methodik verankert ist. Teil der übergeordneten Funktionsarchitektur sind die Fähigkeiten „Merkmale erfassen“, „Merkmale erkennen“, etc. Abweichungen der Fähigkeiten sind rot umrundet. Das Vorgehen wird anhand eines Szenarios mit konkreten Inhalten abgeglichen.

Sicht	**Ebene**	**Analyseinhalt**	**CFT** (↓ Identifikation)		**probFMEA** (↑ Folgerung)	
Verhaltens-sicht	Fahrzeug-verhalten (im Szenario)	Verhaltensabweichungen / -fehler	Top-Level-Event, TLE		mögliche Verhaltensfehler	
Fähigkeiten-sicht	Fähigkeiten	Fähigkeitsdefizite	↓	Welche Fähigkeitsdefizite und -abweichungen, können zu bestimm-ter Verhaltensabweichung führen?	↑	Zu welchen Verhaltensabweichungen führen mögliche Fähigkeitsdefizite?
technische Sicht	Systemstruktur	Schwächen und Abweichungen von beabsichtigter Funktion	↓	Welche funktionalen Schwächen und -abweichungen können zu bestimm-tem Fähigkeitsdefizit führen?	↑	Zu welchen Fähigkeitsdefiziten führen funktionale Schwächen und -abweichungen?
	Einzelbestandteile	Fehler und Versagen von Einzel-elementen, Bauteilen, Software	↓	Durch welche Fehler in Bauteilen und Software kann betreffende Funktionsabweichung entstehen?	↑	Zu welchen Funktionsabweichungen führen mögliche Bauteil- und Softwarefehler?

Abbildung 15: Betrachtete Inhalte je Architekturlevel

Die Inhalte, die je Architekturlevel betrachtet werden, sind in Abbildung 15 gezeigt. Mithilfe des CFT werden vom Top-Level-Event (TLE) ausgehend Defizite und Abweichungen im Verhalten, bei den Fähigkeiten und Fehler bei der technischen Sicht identifiziert. In umgekehrte Richtung setzt die FMEA an, um zu ermitteln, zu welchen Folgerungen die Abweichungen auf den unterschiedlichen Ebenen führen.

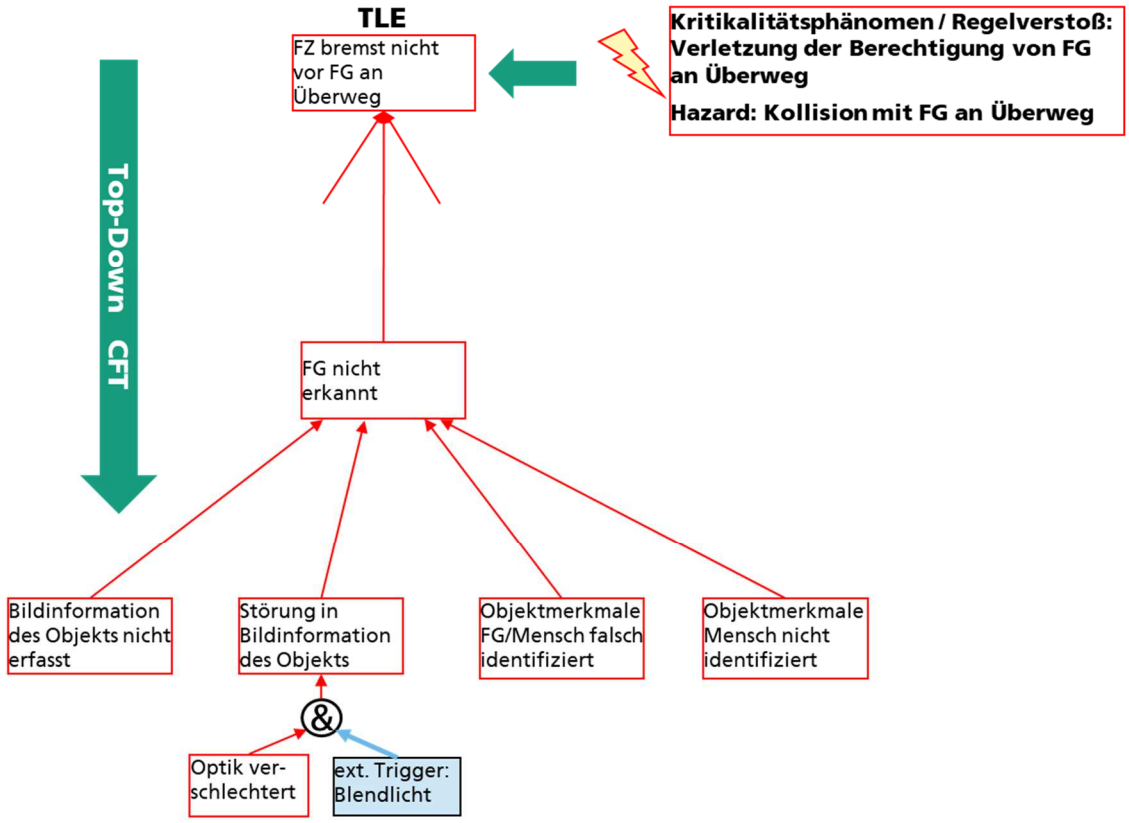


Abbildung 16: Logisches Netzwerk der Kausalbeziehungen von Fehlerursachen und –folgen (Top-Down CFT)

Zum Demonstrieren des Ansatzes wird ein Beispiel verwendet, welches in Abbildung 16 dargestellt ist. Zunächst wird das TLE „Fahrzeug (FZ) bremst nicht vor Fußgänger (FG) an Überweg“ in die Analyse aufgenommen. Dies stellt ein Kritikalitätsphänomen bzw. einen Regelverstoß dar, da die Verletzung der Berechtigung des Fußgängers zum Überqueren des Überwegs verletzt wird. Außerdem liegt ein Hazard vor, der eine mögliche Kollision des Fußgängers mit dem Fahrzeug einschließt. Top-Down wird mittels der CFT nach Ursachen für das Eintreffen des TLE gesucht. Eine Ursache für eine ausbleibende Bremsung kann darin liegen, dass der Fußgänger nicht oder nicht korrekt erkannt wurde. Ein möglicher Grund dafür kann sein, dass eine Störung in der Bildinformation des Objekts aufgrund einer verschlechterten Optik oder dem Auftreten von blendendem Licht vorliegt. Das Blendlicht kann einen externen Trigger darstellen, der nur in Zusammenwirkung mit einer verschlechterten Optik zu einer Störung führt. In umgekehrter Richtung setzt die FMEA an, die innerhalb des Fault-Trees nicht nur die systematische Ermittlung von Fehlerursachen innerhalb der Komponenten durch die Verwendung von HAZOP-Schlüsselwörtern ermöglicht, sondern auch die Ermittlung weiterer TLEs unterstützt, die zu Gefährdungen oder der Verletzung weiterer Sicherheitsziele führen können. Dies ist Abbildung 17 zu sehen ist: Falls ein Objekt fälschlicherweise in der Fahrspur erkannt wurde, kann dies zum einen zu unmotiviertem Bremsen oder je nach Anzahl der Fahrspuren zum unmotivierten Ausweichen auf die Gegenfahrbahn oder Spurwechsel führen.

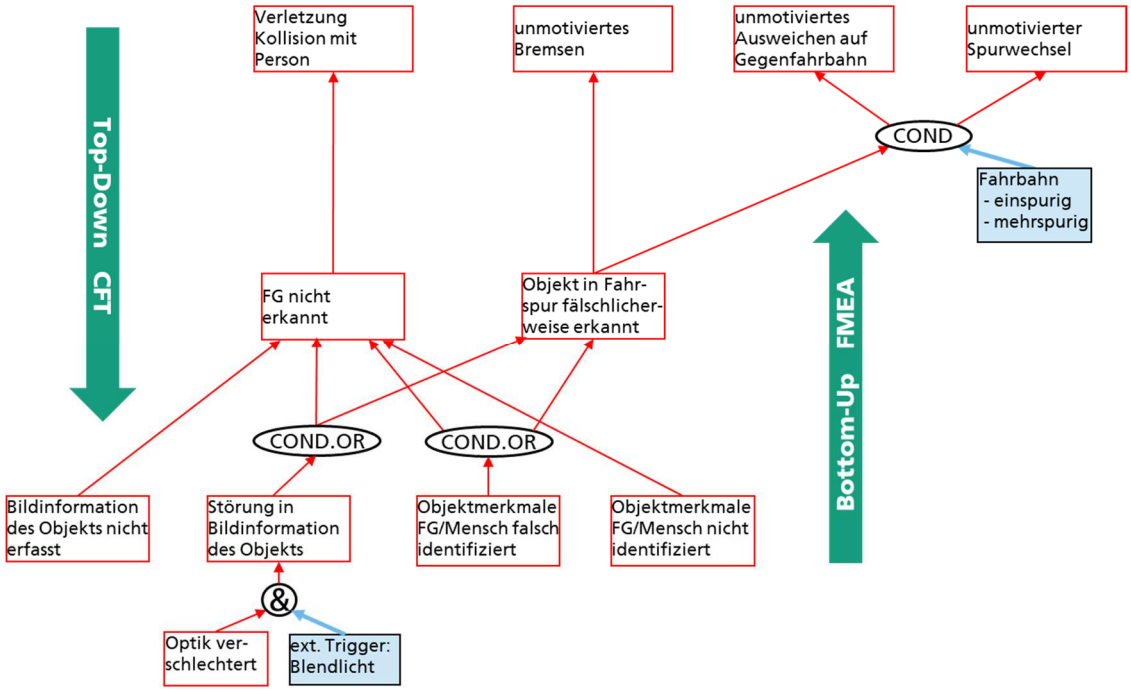


Abbildung 17: Logisches Netzwerk der Kausalbeziehungen von Fehlerursachen und –folgen (Bottom-Up FMEA)

Das resultierende Fehlernetz lässt sich im Rahmen eines CFTs innerhalb von SafeTBox modellieren und in ein offenes Format exportieren. Mittels eines entwickelten Tools, lässt sich der modellierte CFT automatisiert in ein Bayessches Netz transformieren und kann anschließend mittels externer Tools interaktiv quantitativ ausgewertete werden. Die Verwendung des Open Dependability Exchange Meta-Models also Format, lassen sich beliebige Tooladapter einbinden und implementieren. Bei der Modellierung wird hierbei die hinterlegte Fähigkeitenarchitektur als Rankhilfe verwendet. Dies erlaubt es die Nachfolgerbarkeit und Konsistenz zwischen den Komponenten der Architektur und deren Schnittstellen mit dem Fehlermodell zu gewährleisten. Abbildung 18 zeigt beispielhaft den Bezug zwischen Komponententyp und Fehlermodell (CFT) sowie die Zuordnung der Fehler zu den Schnittstellen der Komponenten über die Fehler-Ports (dreieckig) und die Ports der Komponenten (quadratisch) mittels einer gestrichelten Linie.

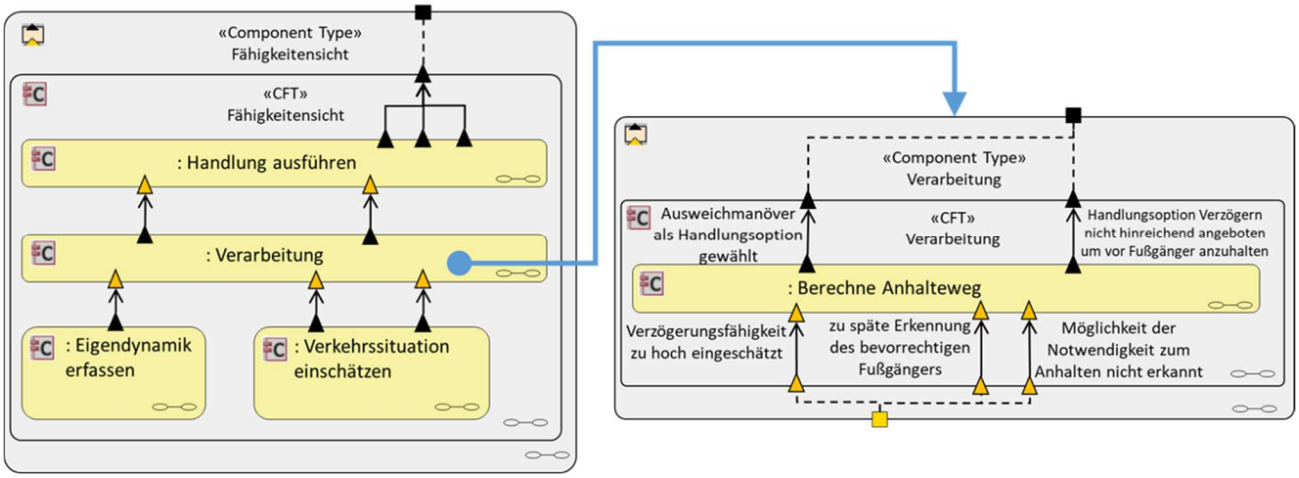


Abbildung 18: Umsetzung in SafeTBox mit hinterlegter Fähigkeitenarchitektur (1/3)

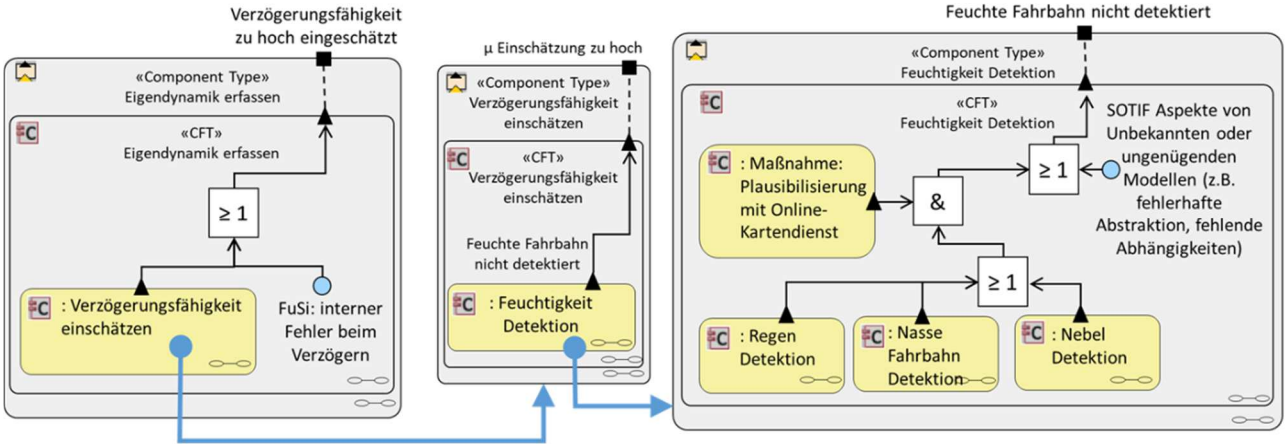


Abbildung 19: Umsetzung in SafeTBox mit hinterlegter Fähigkeitenarchitektur (2/3)

Die Darstellung in Abbildung 19 zeigt die Erweiterung der-CFT Methodik zur Modellierung von SOTIF Aspekten wie *Unknowns* (Abbildung 19, rechts) bzw. Umwelteinflüsse sowie technischen Schwächen. In dem Beispiel ist die Schwäche eines Sensors in Bezug auf die Detektion von Nebel modelliert (Abbildung 20, rechte Seite). In Bezug auf die Modellierung könnten Weaknesses sowohl systematischer als auch technischer Natur sein: Ein Beispiel für eine systematische Schwäche eines neuronalen Netzes ist es nur Muster zu erkennen, welche in den Trainingsdaten hinreichend repräsentiert wurden. Eine technische Schwäche eines Lidar[8]-Sensors sind beispielsweise Reflektionen, wie weiter unten dargestellt.

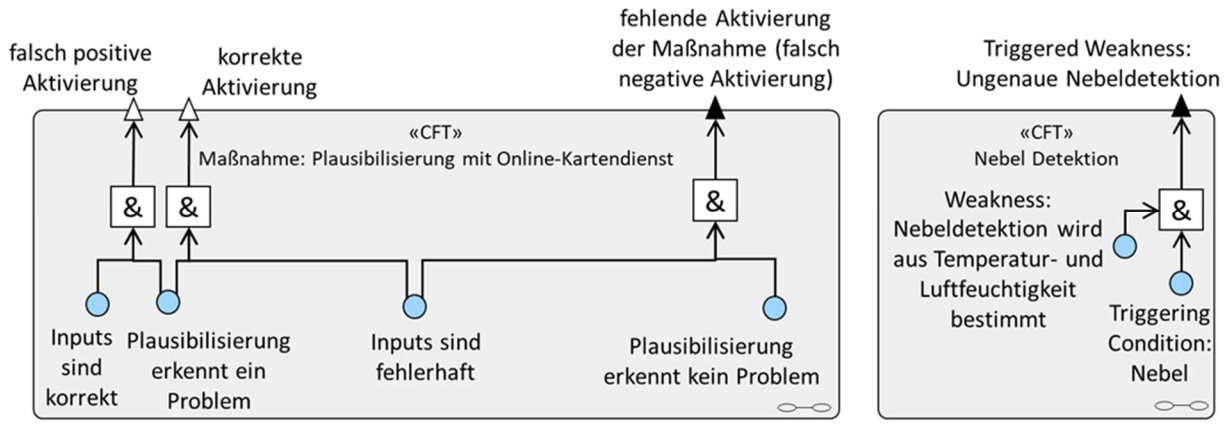


Abbildung 20: Umsetzung in SafeTBox mit hinterlegter Fähigkeitenarchitektur (3/3)

Mit dem hier vorgestellten Ansatz wird eine erweiterte Methodologie zur analytischen Verifikation automatisierter Fahrzeuge ermöglicht. Dies gestattet eine szenarienbezogene Überprüfung des Verhaltens anhand situativ erforderlicher Fähigkeiten. Außerdem lässt sich hiermit eine Analyse von Fähigkeitsmängeln, Komponentenschwächen und –fehlern durchführen in einem Ansatz, der Fehlerbäume und FMEA vereint. Des Weiteren ermöglicht dies eine quantitative Auswertung mit Bayesschen Netzwerken aufbauend auf den Konzepten der probabilistischen FMEA. Um eine quantitative Datenbasis aufzubauen, wird zunächst mit Abschätzungen der Größenordnungen der

[8] Lidar steht für "Light Detection and Ranging" und bedeutet auf Deutsch soviel wie Lichterkennung und Reichweitenmessung. Damit gehört die Technik zur Gattung der ToF-Sensoren. "Time-of-Flight"-Sensoren messen per ausgesendetem Lichtimpuls die Dauer, die das Licht benötigt um zu einem Objekt zu gelangen und wieder zum Sensor zurückzukehren.

Ausfallwahrscheinlichkeiten gearbeitet. Für exaktere Ergebnisse besteht jedoch der Wunsch, dass eine evolutionäre, branchenweite Datenerhebung stattfindet. Bezüglich der Umsetzbarkeit und Anwendbarkeitsoptimierung besteht im Projekt die Möglichkeit, den Ansatz innerhalb des VVM-Projekts zu erproben. Im Zuge dieses Bestrebens werden die Anforderungen an die Methodik und die entsprechenden Arbeitsumgebungen ermittelt.

Der hier beschriebene Ansatz hat einen AP-übergreifenden Charakter, aber wird überwiegend in AP4.1 verortet. Im kommenden Berichtszeitraum wird ausgehend von diesem Ansatz ein Beispiel anhand der Functional Use Cases entwickelt.

Anbindung im Assurance Framework und den Risk Management Core

Im Projektverlauf wurden Anbindungspunkte der Methodik ins Gesamtprojekt bzw. des Assurance Framework, welches auf Abbildung 21 zu sehen ist, und den Risk Management Core identifiziert.

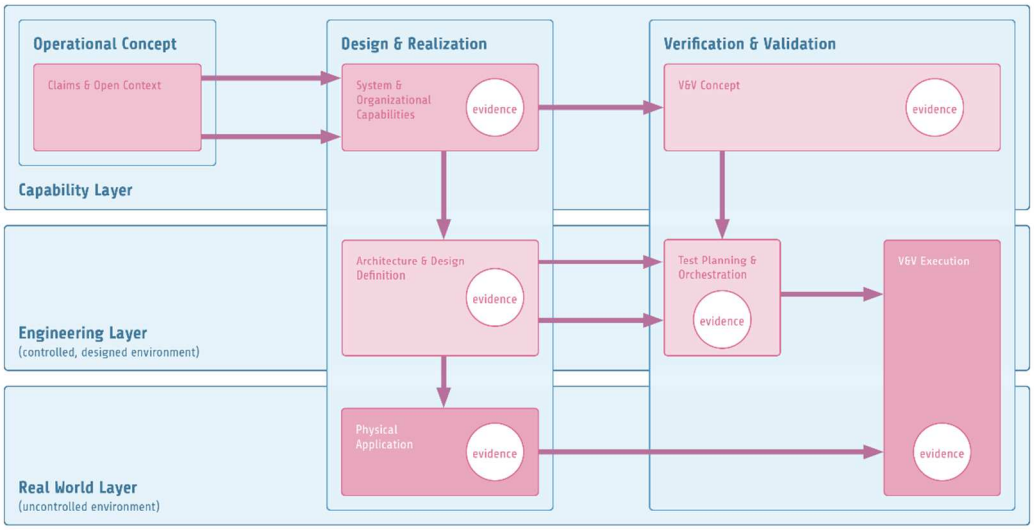


Abbildung 21: VVM Assurance Framework

Ein Arbeitsstand der probFMEA/CFT-Methodik und ihrer Anbindung an das Assurance Framework ist in Abbildung 22 zu sehen. Die Methodik bezieht ihren Input u.a. aus den Sicherheitsanforderungen im Functional Use Case und der Architektur (funktional/technisch). Ein Output der Methodik ist es, Evidenzen für die Sicherheitsargumentation bzw. Assurance Argumentation bereitzustellen.

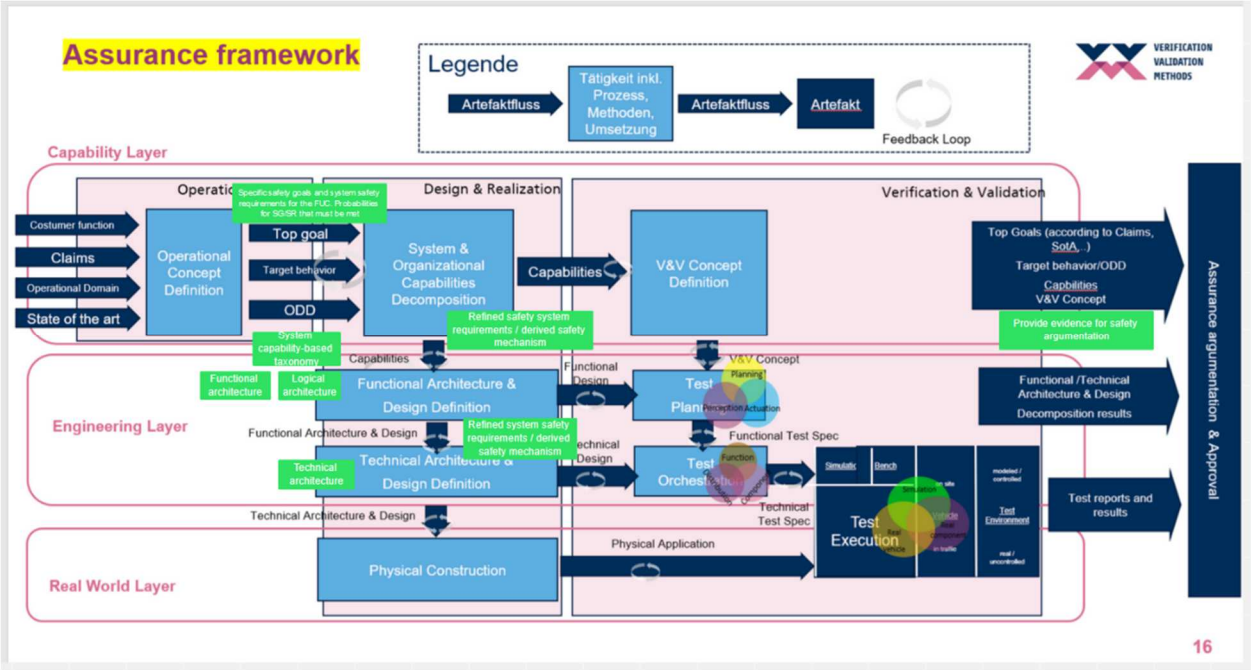


Abbildung 22: Anbindung der Methodik an Assurance Framework

Neben der Verortung der Methodik im Assurance Framework, wurden auch erste Anknüpfungspunkte der Methodik an den Risk Management Core vorgenommen.

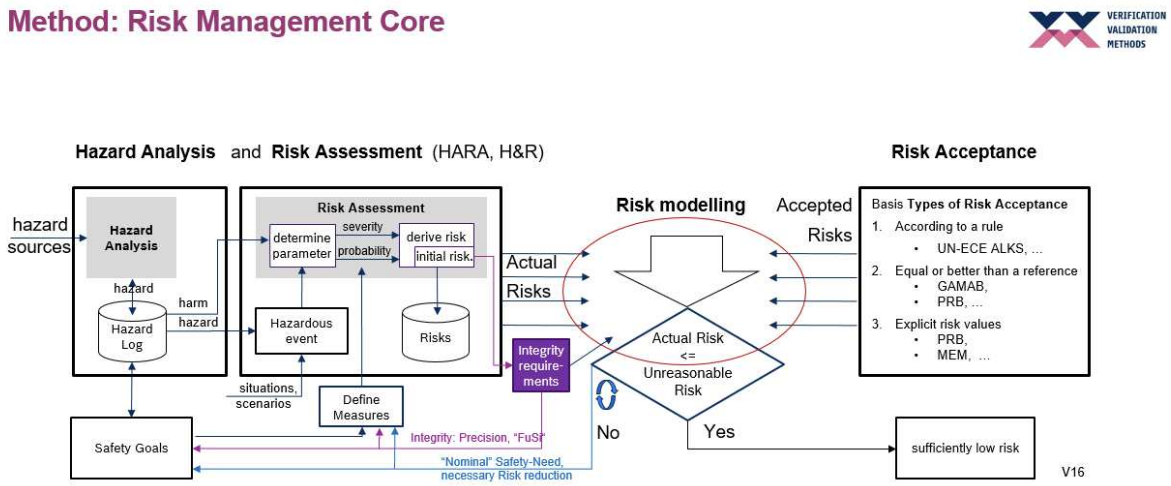


Abbildung 23: Schnittstellen und Übergabeartefakte des Risk Management Core

Das Schema des Risk Management Core ist auf Abbildung 23 abgebildet. Ein wichtiger Input aus dieser AG ist die Ermittlung der Wahrscheinlichkeiten, die einen elementaren Bestandteil für die Methodik der probFMEA/CFT darstellen. Neben den Wahrscheinlichkeiten kann die Methodik auch abbilden, ob die Sicherheitsziele des Systems eingehalten werden.

Argumentationsframework

Ein bedeutender Beitrag des Fraunhofer IESE war die Leitung von Core03 und die Erstellung einer konsistenten Gesamtprojektargumentation. Es wurden mehrere Face-to-Face-Workshops in

Kaiserslautern ausgerichtet, um die Abstimmung mit allen relevanten internen und externen Stakeholdern zu koordinieren. Zudem wurde eine Präsentation für den projektübergreifenden Block des Halbzeitevents zur Sicherheitsargumentation vorbereitet und in München gehalten.

Weitere bedeutende Aktivitäten umfassten die Teilnahme an einer Panel-Diskussion mit internationalen Experten sowie die Mitwirkung an einem ATZ-Zeitschriften-Beitrag zum Thema „Absicherungsmethoden für komplexe Verkehrsszenarien zur Freigabe automatisierter Fahrfunktionen“. (https://link.springer.com/article/10.1007/s35148-022-0898-0) Die Ergebnisse und Methoden wurden auf verschiedenen internationalen Workshops und Symposien, wie dem safeCAD-DJ Symposium in Berlin und dem SIP-ADUS Workshop in Kyoto, Japan, präsentiert.

Die Kernergebnisse von Core03, die unter Führung des IESE im Berichtszeitraum erreicht wurden, umfassen die Integration des Risk Management Core Konzeptes in die projektübergreifende Sicherheitsargumentation, die Methoden zur Ableitung des sicheren Sollverhaltens, die Integration der Methoden des Szenarienstrangs sowie die Testplanung und Testorchestrierung in die Sicherheitsargumentation. Diese Ergebnisse wurden in einem GSN-konformen Modell der Sicherheitsargumentation dargestellt und auf dem Final Event präsentiert. Zudem wurden mehrere Poster erstellt, die die Sicherheitsargumentation auf dem Final Event vorstellten und die umfassende und explizite Begründung der ADS-Sicherheit zeigten.

1.1.2.2 AP4.2 – Definition von Systemanforderungen

Im Arbeitspaket AP4.2 lag der Fokus der FhG auf der Weiterentwicklung und Anwendung der in AP4.1 entwickelten Methodik zur funktionalen Sicherheit im Szenarioraum Urbane Kreuzung. Ein wesentlicher Beitrag war die risikobasierte Ableitung von Systemanforderungen.

Die Systemanforderungen wurden in einem konsolidierten Katalog zusammengeführt und anhand ausgewählter konkreter Beispiele validiert. Hierbei wurde die Praktikabilität bewertet und mögliche Restriktionen analysiert. Aufgrund der Wichtigkeit der Sicherheitsargumentation wurden die ursprünglich geplanten Arbeiten zum dynamischen Risikomanagement zugunsten der Weiterentwicklung der Sicherheitsargumentation umverteilt. Diese Anpassung wurde im Zwischenbericht beschrieben und ermöglichte es, die Ressourcen auf die dringend benötigte Sicherheitsargumentation zu konzentrieren.

Ableiten von Systemanforderungen mit dem Null-Design

Neben der gemeinsamen Arbeit des IESE und LBF an der in AP 4.1 beschriebenen Methodik nahmen beide Institute aktiv an den regelmäßigen Arbeitstreffen der AG6 teil. Die Arbeitsgruppe hat sich das Ziel gesetzt, exemplarische Systemanforderungen inkl. Gütekriterien zu formulieren. Grundlage der Arbeiten ist das Nulldesign (Top Down), welches in AP3.4 erarbeitet wurde und die Ergebnisse der TP7 AG7 „Validierung Sensormodelle“ (Bottom Up). In der AG sollte eine Verbindung zwischen den beiden Ansätzen gefunden werden und bestehende Lücken sollen geschlossen werden.

Output dieser Arbeitsgruppe sind unter anderem eine exemplarische Logische Architektur und Systemanforderungen, die als Input für die probFMEA-/CFT-Methodik benötigt werden. Im Folgenden werden die wesentlichen Ergebnisse, die unter Mitwirkung der FhG entstanden,

zusammengefasst (vgl. auch zusammenfassender Abschlussbericht, wo diese Ergebnisse ebenfalls einflossen):

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,
- Behavioral Safety Requirements spezifizieren lösungsunabhängiges sicherheitsrelevantes Verhalten oder lösungsunabhängige Sicherheitsmaßnahmen einschließlich ihrer sicherheitsrelevanten Eigenschaften

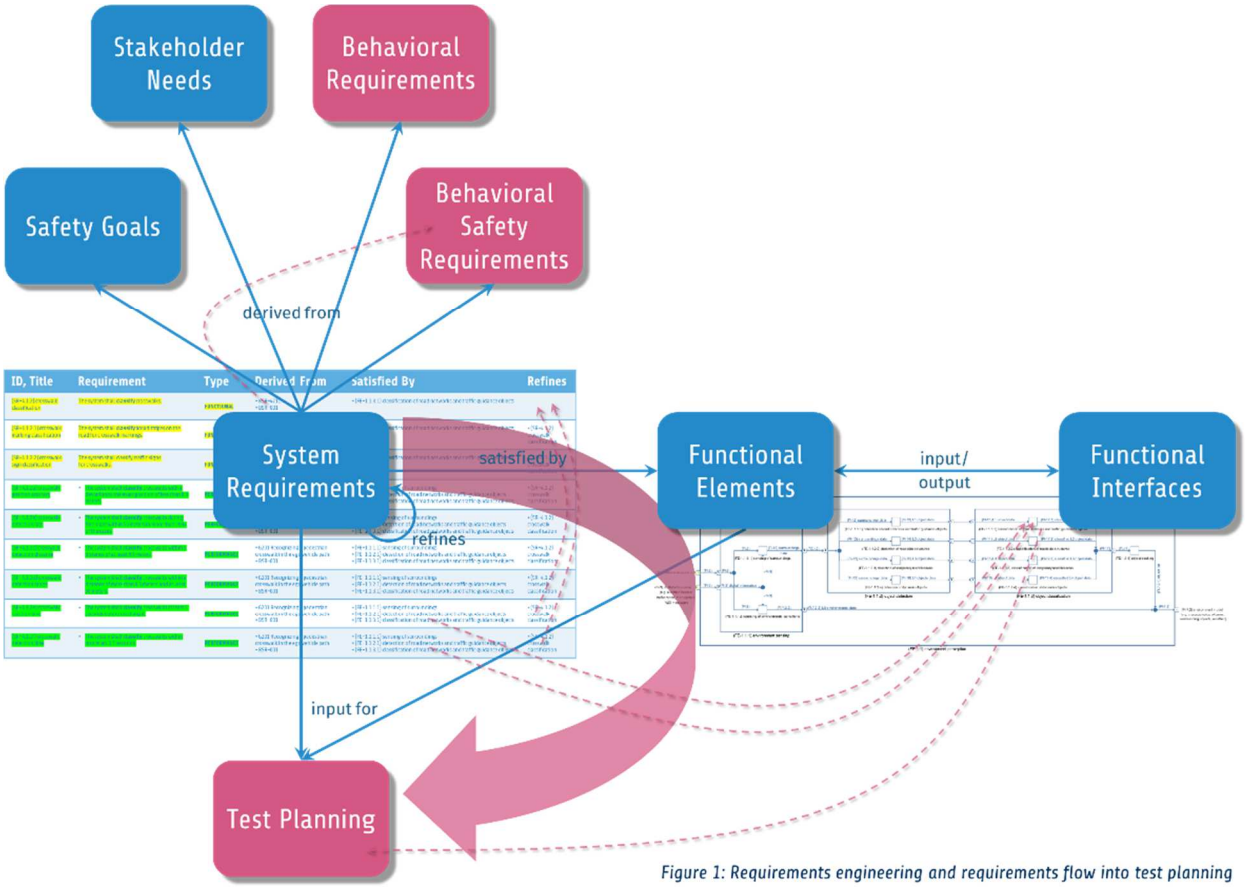


Abbildung 24: Zusammenhang zwischen Testplanung, Safety Goals und Requirements (Bild entstand in Zusammenarbeit der Partner im TP4 durch Partner ZF)

Übergabe an die Testplanung

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, die in AP 4.1 beschrieben wurde, 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.
- Leistungsanforderungen sind messbare Kriterien, die angeben, [...] wie gut die funktionalen Anforderungen erfüllt werden sollen.

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.

1.1.2.3 AP4.3 – Definition von Testanforderungen

Das LBF beteiligte sich an der Erstellung der funktionalen Testplanung. Diese ist notwendig zur Vorbereitung des wesentlichen Übergabeartefakt an die Testorchestrierung, die Funktionale Testspezifikation, welche im Deliverable 06 vorgestellt werden konnte.

Testplanung

In dem Zuge wurde zunächst die Testplanung in Relation zur nachgeschalteten Testorchestrierung (TP7) gesetzt, siehe Abbildung 25:

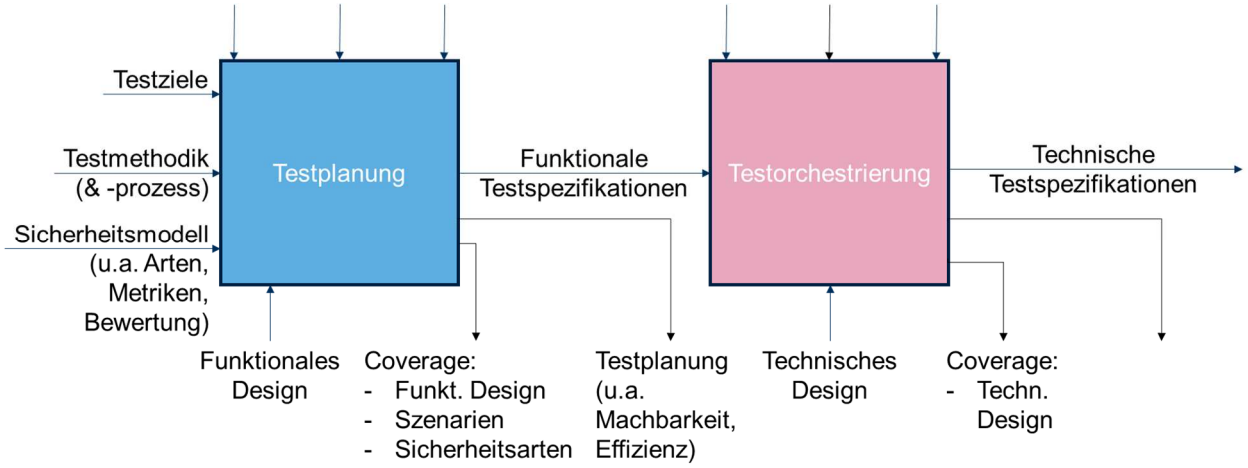


Abbildung 25: Zusammenhang von Testplanung und Testorchestrierung, sowie vollständige IN/Output-Struktur

Die Testplanung selbst wurde im Folgenden verfeinert und die komplette I/O-Struktur erarbeitet, Abb. 26:

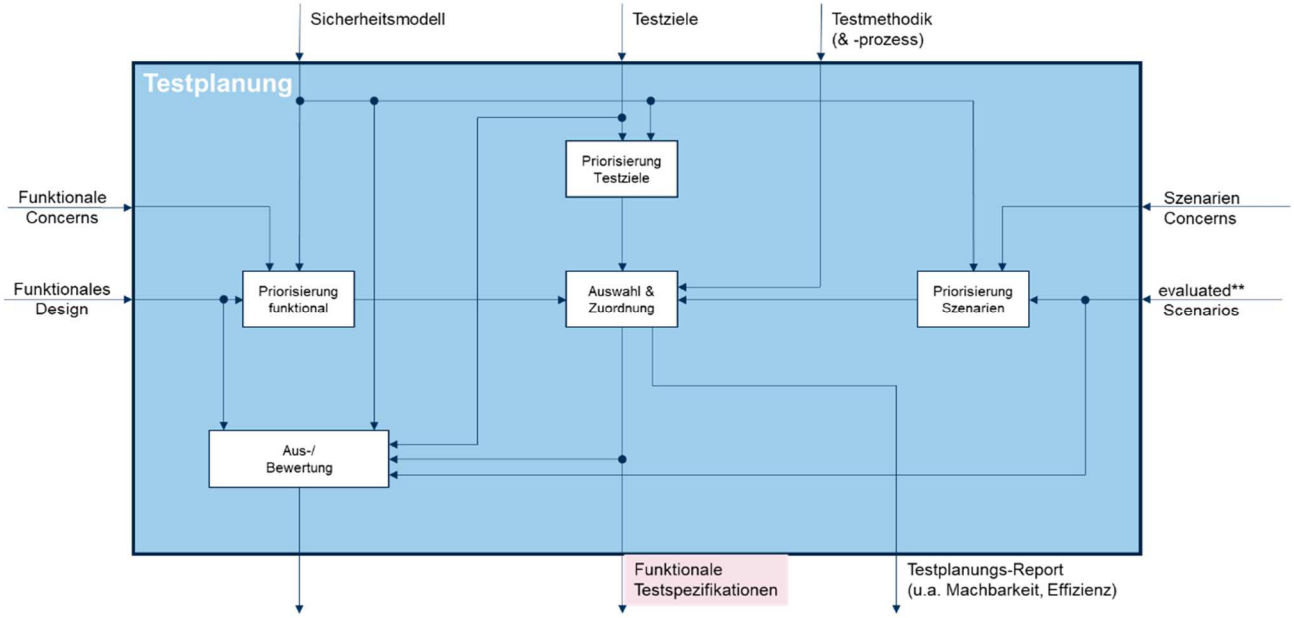


Abbildung 26: Detaildarstellung der Testplanung

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.

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 deren Qualitäten.

Der bisher skizzierte Kernprozess der Testplanung befasst sich mit der Erstellung einzelner Testspezifikationen. Durch wiederholte Anwendung entsteht eine Gesamtmenge von Testspezifikationen, die, wie oben erwähnt, jeweils nur einen begrenzten Testraum abdecken kann. Für die Argumentation ist es von großer Bedeutung, die Abdeckung dieses Testraums beurteilen zu können. Da das funktionale Design, die Szenarien und die verschiedenen Arten von Sicherheit in Testfällen verknüpft wurden, muss die Aussage zur Testabdeckung immer alle 3 Dimensionen umfassen. Andere Kriterien wie Durchführbarkeit und Effizienz stehen im Widerspruch dazu. Sie stehen in direktem Zielkonflikt mit der möglichst hohen Testabdeckung und vervollständigen das Bild, inwieweit diese Anforderungen an das Testkonzept auch erfüllt werden.

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 27 zeigt das konkrete Beispiel einer in VVM entworfenen funktionalen Prüfvorschrift für die Verifikation.

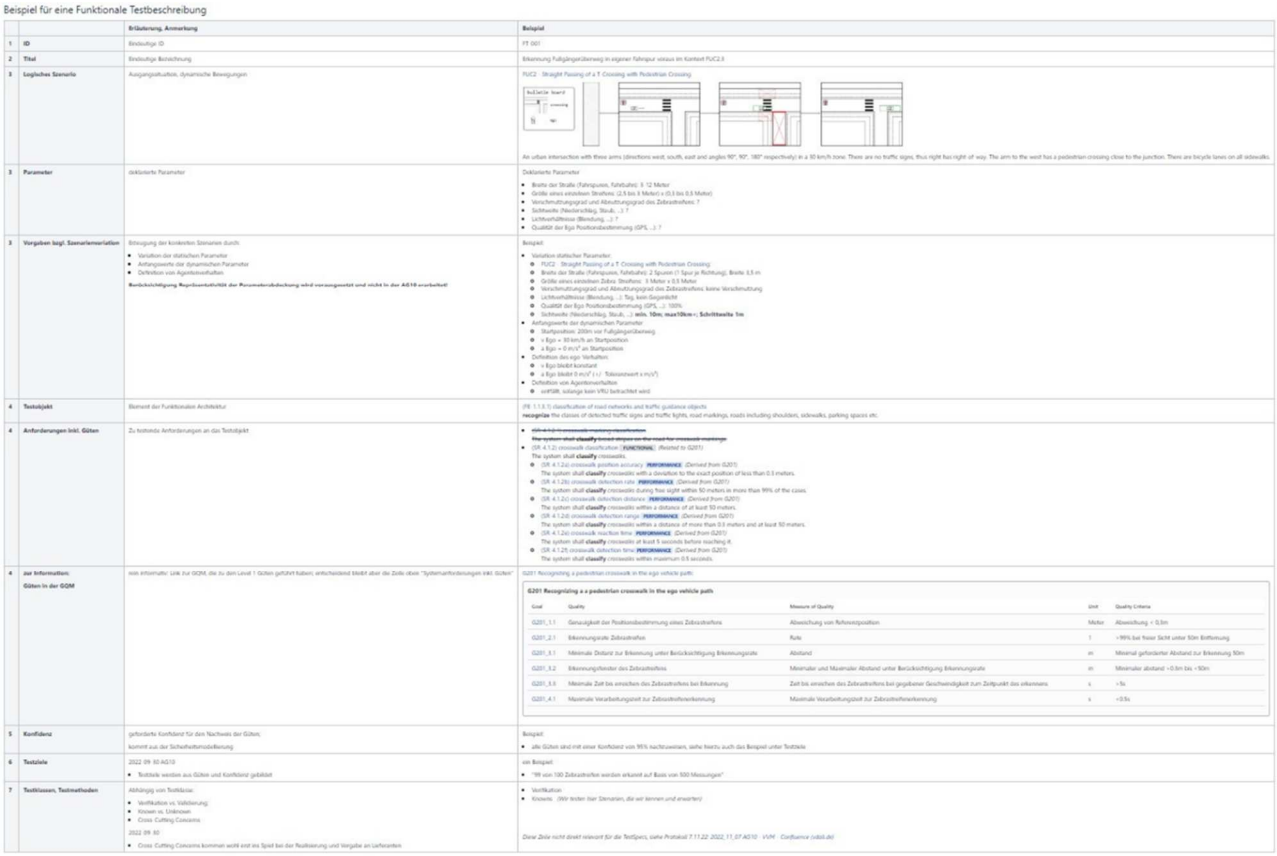
Nach dem Identifikator und der eindeutigen Bezeichnung der funktionalen Testspezifikation werden über die nächsten Attribute die Testszenarien beschrieben. Dabei sind zwei Informationen wesentlich: das logische Szenario und die Variationsregel. Zunächst wird das zugrundeliegende funktionale Szenario 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. Implizit werden an dieser Stelle Testabbruchkriterien für den Fall angegeben, dass ein Testziel aufgrund unzureichender Performance nicht erreicht werden kann.


Beispiel für eine Funktionale Testbeschreibung

		Erläuterung, Anmerkung	Beispiel
1	ID	Eindeutige ID	FT 001
2	Titel	Eindeutige Benennung	Erkennung Fußgängerüberweg in eigener Fahrspur voraus im Kontext FUC2.1
3	Logisches Szenario	Ausgangssituation, dynamische Bewegungen	FUC2 - Straight Passing of a T Crossing with Pedestrian Crossing An urban intersection with three arms (directions west, south, east and angles 90°, 90°, 180° respectively) in a 30 km/h zone. There are no traffic signs, thus right has right-of-way. The arm to the west has a pedestrian crossing close to the junction. There are bicycle lanes on all sidewalks.
3	Parameter	deklarierte Parameter	Deklarierte Parameter • Breite der Straße (Fahrspuren, Fahrbahn): 3 .12 Meter • Größe eines einzelnen Streifens: (2,5 bis 3 Meter) x (0,3 bis 0,5 Meter) • Verschmutzungsgrad und Abnutzungsgrad des Zebrastreifens: ? • Sichtweite (Niederschlag, Staub, ...): ? • Lichtverhältnisse (Blendung, ...): ? • Qualität der Ego Positionsbestimmung (GPS, ...): ?
3	Vorgaben bzgl. Szenariovariation	Bildung der konkreten Szenarien durch: • Variation der statischen Parameter • Anfangswerte der dynamischen Parameter • Definition von Agentenverhalten **Berücksichtigung Repräsentativität der Parametrisierung wird vorausgesetzt und nicht in der AG10 erarbeitet!**	Beispiel: • Variation statischer Parameter: ○ FUC2 - Straight Passing of a T Crossing with Pedestrian Crossing ○ Breite der Straße (Fahrspuren, Fahrbahn): 2 Spuren (1 Spur je Richtung), Breite 6,5 m ○ Größe eines einzelnen Zebra Streifens: 3 Meter x 0,5 Meter ○ Verschmutzungsgrad und Abnutzungsgrad des Zebrastreifens: keine Verschmutzung ○ Lichtverhältnisse (Blendung, ...): Tag, kein Gegenlicht ○ Qualität der Ego Positionsbestimmung (GPS, ...): 100% ○ Sichtweite (Niederschlag, Staub, ...): **min. 10m, max10km+; Schrittweite 1m** • Anfangswerte der dynamischen Parameter ○ Startposition: 200m vor Fußgängerüberweg ○ v Ego = 30 km/h an Startposition ○ a Ego = 0 m/s² an Startposition • Definition des ego Verhalten: ○ v Ego bleibt konstant ○ a Ego bleibt 0 m/s² (+/- Toleranzwert x m/s²) • Definition von Agentenverhalten ○ entfällt, solange kein VRU betrachtet wird
4	Testobjekt	Element der Funktionalen Architektur	(FR 1.1.1.1) classification of road networks and traffic guidance objects **recognize** the classes of detected traffic signs and traffic lights, road markings, roads including shoulders, sidewalks, parking spaces etc.
4	Anforderungen inkl. Güten	Zu testende Anforderungen an das Testobjekt	~~(SR 4.1.1) crosswalk mystery classification~~ ~~The system shall classify traced objects on the road for crosswalk markings~~ • (SR 4.1.2) crosswalk classification (**FUNCTIONAL**, *Related to G201*) The system shall **classify** crosswalks. ○ (SR 4.1.2a) crosswalk position accuracy (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks with a deviation to the exact position of less than 0.5 meters. ○ (SR 4.1.2b) crosswalk detection rate (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks during fog: sight within 50 meters in more than 99% of the cases. ○ (SR 4.1.2c) crosswalk detection distance (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks within a distance of at least 50 meters. ○ (SR 4.1.2d) crosswalk detection range (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks within a distance of more than 0.5 meters and at least 50 meters. ○ (SR 4.1.2e) crosswalk reaction time (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks at least 5 seconds before reaching it. ○ (SR 4.1.2f) crosswalk detection time (**PERFORMANCE**, *Derived from G201*) The system shall **classify** crosswalks within maximum 0.5 seconds.
4	zur Information: Güten in der GDM	nicht informativ: Link zur GDM, die zu dem Level 1 Gütein geführt haben; entscheidend bleibt aber die Ziele oben "Systemanforderungen inkl. Güten"	G201 Recognizing a pedestrian crossway in the ego vehicle path **G201 Recognizing a a pedestrian crossway in the ego vehicle path** Goal / Quality / Measure of Quality / Unit / Quality Criteria G201_1.1 Genauigkeit der Positionsbestimmung eines Zebrastreifens / Abweichung von Referenzposition / Meter / Abweichung < 0,5m G201_2.1 Erkennungsrate Zebrastreifen / Rate / ? / >99% bei freier Sicht unter 50m Entfernung G201_3.1 Minimale Distanz zur Erkennung unter Berücksichtigung Erkennungsrate / Abstand / m / Minimal geforderter Abstand zur Erkennung 50m G201_3.2 Erkennungsfenster des Zebrastreifens / Minimaler und Maximaler Abstand unter Berücksichtigung Erkennungsrate / m / Minimaler abstand <0.5m bis >50m G201_3.3 Maximale Zeit bis erreichen des Zebrastreifens bei Erkennung / Zeit bis erreichen des Zebrastreifens bei gegebener Geschwindigkeit zum Zeitpunkt des erkennens / s / >5s G201_4.1 Maximale Verarbeitungszeit zur Zebrastreifenerkennung / Maximale Verarbeitungszeit zur Zebrastreifenerkennung / s / <0.5s
5	Konfidenz	geforderte Konfidenz für den Nachweis der Güten; kommt aus der Sicherheitsmodellierung	Beispiel: • alle Güten sind mit einer Konfidenz von 95% nachzuweisen, siehe hierzu auch das Beispiel unter Testziele
6	Testziele	2022 09 30 AG10 • Testziele werden aus Güten und Konfidenz gebildet	ein Beispiel: • "99 von 100 Zebrastreifen werden erkannt auf Basis von 500 Messungen"
7	Testklassen, Testmethoden	Abhängig von Testklasse: • Verifikation vs. Validierung • Known vs. Unknown • Cross Cutting Concerns 2022 09 30 • Cross Cutting Concerns kommen wohl erst ins Spiel bei der Realisierung und Vergabe an Lieferanten	• Verifikation • Knowns (Wir testen über Szenarien, die wir kennen und erwarten) *Diese Ziele nicht direkt relevant für die TestSpecs, siehe Protokoll 7.11.22 2022_11_07 AG10 - VVM - Confluence (vdali.de)*

Abbildung 27: 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 28 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.

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 (stroggenommen sind Validierungs-Maße gemeint)	Es muss nachgewiesen werden, welche Sicherheitsreserve im Falle einer Kollisionsvermeidung besteht. As 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 0,3 (30% 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	Bsp: • Kameramaterial/Bildaufzeichnungen • Daten aus dem Ego-Fahrzeug zu o Bewegung o Umfeld o etc.

Abbildung 28: Beispielhafte Funktionale Testspezifikation für die Validierung

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 29 stellt den Zusammenhang zwischen Testplanung und Testorchestrierung dar und zeigt die relevanten Inputs.

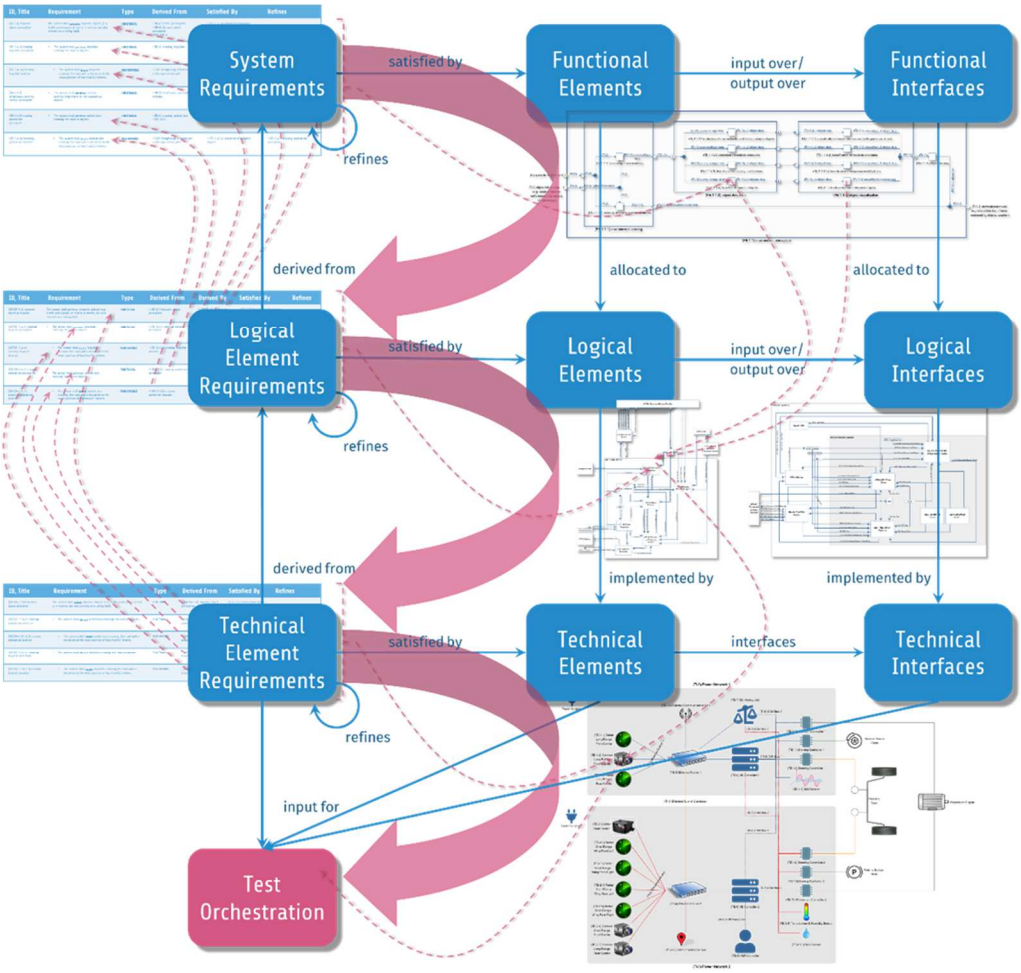


Abbildung 29: Inputs für die Testorchestrierung (Bild entstand in Zusammenarbeit der Partner im TP4 durch Partner ZF)

1.1.3 TP6

1.1.3.1 Auswahl und Vorbereitung der Messstellen

Die Auswahl geeigneter Messstellen war eine zentrale Aufgabe, die in Zusammenarbeit mit der Verkehrsunfallforschung an der TU Dresden GmbH (VUFO) durchgeführt wurde. Eine Unterarbeitsgruppe, an der das Fraunhofer IVI beratend teilnahm, traf die Auswahl der Messstellen. Diese Auswahl basierte auf Unfallstatistiken und weiteren relevanten Verkehrsdaten. Dabei beriet das Fraunhofer IVI die VUFO sowohl in den initialen Treffen der Unterarbeitsgruppe als auch in bilateralen Gesprächen bei der Auswahl geeigneter Messpunkte. Parallel dazu wurden die notwendigen Unterlagen für die Beantragung der Messungen bei den Behörden vorbereitet.

1.1.3.2 Installation und Betrieb der Messtechnik

Die Messtechnik, bestehend aus Infrarotkameras (Wärmebild) und entsprechenden Bildanalysealgorithmen, wurde vom Fraunhofer IVI vorbereitet. Dies umfasste die Kalibrierung der Kameras und die Entwicklung der Algorithmen zur Erfassung und Analyse der Verkehrssituationen.

Die Messstellenvorschläge wurden im März 2021 von der VUFO erhalten. Es folgten Anfragen nach Leitungskarten bei der Stadt Dresden im April 2021, der Erhalt dieser Karten im Juni 2021 und die

endgültige Festlegung der Messstellen im Juli 2021. Die Genehmigungen der Messungen wurden bei den zuständigen Behörden beantragt.

Die Installation der Messtechnik an den verschiedenen Messstellen erfolgte wie folgt:

- Erste Messstelle (Tharandter Straße): Die Messtechnik wurde an einer Straßenlaterne in einer Höhe von 4,63 m angebracht. Die Erfassung begann am 09.09.2021 und dauerte bis zum 07.10.2021. Insgesamt wurde 656 Stunden verwertbares Videomaterial aufgezeichnet.
- Zweite Messstelle (Zamenhofstraße/Robert-Berndt-Straße/Hertzstraße): Die Installation erfolgte am 07.10.2021 und dauerte bis zum 15.11.2021. Hier traten technische Probleme und Vandalismus auf, die die Datenerfassung beeinträchtigten. Trotzdem konnten 197 Stunden verwertbares Videomaterial aufgezeichnet werden.
- Dritte Messstelle (Budapester Straße): Nach der Genehmigung am 02.06.2022 wurde die Messtechnik am 08.06.2022 installiert und bis zum 15.07.2022 betrieben. So konnten 838 Stunden verwertbares Videomaterial aufgezeichnet werden.

1.1.3.3 Datenerfassung und -analyse

Während der Messungen wurden regelmäßige Wartungsarbeiten durchgeführt, um die fehlerfreie Funktion des Systems sicherzustellen. Dies umfasste das Auswechseln von Datenspeichern und Akkumulatoren. An den drei Messstellen wurden insgesamt 1691 Stunden Videomaterial aufgezeichnet. Die aufgezeichneten Videodaten wurden mit bildverarbeitenden Algorithmen analysiert. Diese Algorithmen wurden im Laufe des Projekts weiterentwickelt und an die spezifischen Anforderungen angepasst. Die Bildverarbeitung umfasste die Identifizierung von Trajektorien und Geschwindigkeiten der Verkehrsteilnehmer.

Die Ergebnisse umfassten detaillierte Trajektorien und Geschwindigkeiten der erfassten Verkehrsteilnehmer. Diese Daten wurden im Fraunhofer IVI F-JSON Format kodiert und zusammen mit einem Codebook bereitgestellt. Die Auswertung der Daten dauerte bis Ende November 2022, sodass die Ergebnisse zum Abschluss des zweiten Halbjahres 2022 präsentiert und an TP8 übergeben werden konnten.

1.1.3.4 Herausforderungen und Verzögerungen

Die Covid-19-Pandemie führte zu Einschränkungen in der Laborarbeit und verzögerte den Aufbau der Systeme. Außerdem wurden die behördlichen Genehmigungen langsamer als erwartet erteilt, was ebenfalls zu Verzögerungen führte. Insbesondere an der zweiten Messstelle traten technische Probleme und Vandalismus auf, die die Datenerfassung beeinträchtigten.

1.1.4 TP 7

1.1.4.1 AP7.1 Anforderungsanalyse

Die Arbeitsschwerpunkte des LBF im Rahmen des Arbeitspaketes *TP7.1 Anforderungsanalyse* bestanden in der Aufbereitung und Darstellung des **Stands der Technik bei Testinfrastrukturen** mit einem Fokus auf das Testen mechatronischer Systeme und XiL-Konzepten. Im Rahmen einer ersten Abstimmung der Teilprojektpartner wurden die drei prinzipielle Testmittel der Simulation, eines Komponententests sowie der reale Fahrversuch identifiziert. Hierbei migrieren XiL-Methoden Artefakte sowohl aus der Simulation (virtuelle Repräsentation eines Restsystemverhaltens) sowie aus dem Komponententest, der eine reale Komponente als Prüfling beinhaltet. Bei einem mechatronischen System können dabei sowohl Informationssignale, elektrische Größen und/oder

mechanische Erregungen zwischen der realen Komponente und einer virtuellen Restsystemsimulation ausgetauscht werden. Werden leistungselektrische oder mechanische Schnittgrößen ausgetauscht, sind entsprechende Leistungsschnittstellen zwischen virtueller und realer Welt vorzusehen. Die Arbeiten wurden im *Schnellboot 5 – Aufsatzpunkt TP7 Testmittel: Fahrzeug, Modelle, System under Test* weitergeführt, bei dem das LBF ein erstes Konzept für eine XiL-Prüfung vibrationsempfindlicher Komponenten vorstellte. Die prinzipiell realisierbaren Testmöglichkeiten eines xIL-Prüfstandes zur Nachbildung von Fahrzeugbewegungen und –vibrationen wurden ebenso wie der Stand der Technik im Bereich XiL in Confluence beschrieben (https://confluence.vdali.de/pages/viewpage.action?pageId=32867986&preview=/32867986/32868157/VVM%20AP7.1%20Stand_der_Technik%20E7.1a%20Fraunhofer%20LBF%20Beitrag.docx; https://confluence.vdali.de/x/OINv).

Im Zuge der weiteren Arbeiten beteiligte sich das LBF aktiv an der Arbeitsgruppe, indem es Informationen über die Aktivitäten im Rahmen des Projekts und mögliche Verbindungen zu Partnerthemen bereitstellte. Ausgangspunkt für die Aktivitäten dieser Phase war die Präsentation der Übersicht über die verfügbaren Testinstanzen, Testmethoden und Testmittel, die sich aus den Arbeiten der einzelnen Partner ergeben. Um eine nachvollziehbare Darstellung der Beiträge zu erreichen, wurde ein MIRO-Board[9], das den gesamten Prozessablauf abbildet, für die Zuordnung der Beiträge der einzelnen Partner in Bezug auf Methoden und Werkzeuge erstellt. Ziel dieser Arbeit war es, die Inhalte, Gemeinsamkeiten, Schnittstellen und Lücken zwischen den verschiedenen Beiträgen klar zu identifizieren. Das Fraunhofer LBF platzierte seinen methodischen Beitrag in der Tabelle "Testdurchführung"[10] des Projektprozesses. Der Beitrag betrifft die Nachbildung realistischer mechanischer Schwingungen auf Sensoren (z.B. LIDAR, Kamera etc.) für AD-Funktionen durch einen x-in-the-Loop-Prüfstand. Die einzelnen bestehenden Arbeitsgruppen im Bereich der Testwerkzeuge betrachten dabei Tests auf Fahrzeugebene, im Fahrzeugerprobungen im Prüfgelände sowie im Rahmen von Simulationen und HIL-Tests. Ferner existiert eine Arbeitsgruppe zur Bündelung der Aktivitäten im Bereich der Co-Simulation. Das Fraunhofer LBF nimmt dabei aktiv an den Arbeitsgruppen zur HIL-Prüfung und Co-Simulation teil.

Ein weiterer Arbeitsschwerpunkt lag in der **Anforderungsanalyse** mit Hinblick auf die Orchestrierung und Umsetzung von Testkonfigurationen. Zu Projektbeginn beteiligte sich das LBF an der Erarbeitung einer Einschätzung zu den Fragen, welche Herausforderungen und Erwartungen beim Test von Level4/5-Systemen bestehen. Die Umsetzung von XiL-Konzepten unterstützt dabei die Forderung nach einem beherrschbaren Testaufwand sowie der Möglichkeit entsprechende Umfänge des Testraums auf Basis einheitlicher Testbeschreibungen abzubilden. Im Zuge der weiteren Arbeiten beteiligte sich das LBF am Schnellboot 1 – Schnittstelle zu AP4, um Anforderungen aus Sicht der VVM-Methodik an Testeinrichtungen abzustimmen. . Im Zuge der regelmäßig stattfindenden Web-Meetings wurden dabei ein gemeinsames Verständnis der Testfallgenerierung und Umsetzung möglicher Testmittel erarbeitet und Schnittstellen in Anlehnung an die VDI2206 Entwurfsmethoden mechatronischer Systeme identifiziert. Hierbei greift die Norm ebenfalls unterschiedliche Testinstanzen (wie Simulationen, Komponentenprüfstände oder Fahrzeugversuche) auf. Im Zuge der fortlaufenden Arbeiten im Rahmen des Schnellboots erfolgt in einem nächsten Schritt die tiefergehende Beschreibung der einzelnen Prozessschritte in der Form einer Prozessbeschreibung, die neben den Ein- und Ausgängen eines dedizierten Prozessschritts

[9] https://miro.com/app/board/o9J_lRCKpz8=/
[10] https://confluence.vdali.de/display/VVM/Schwerpunkte+der+Projektpartner

ebenfalls die eigentlichen Teilprozessschritte beschreibt. Die Arbeiten hierzu wurden in AP7.2 weitergeführt.

1.1.4.2 AP7.2 Entwicklung von Testprozessen und Methoden

Im Rahmen des *TP7.2 Entwicklung von Testprozessen und Methoden* leistete das LBF einen Beitrag zu den gemeinsamen Arbeitsschwerpunkten hinsichtlich der Bewertung von Testmitteln und Ergebnissen, der Konzeptionierung von Testinfrastrukturen und dem Nachweis über das Erreichen von Testzielen, wobei das LBF spezifische Kompetenzen auf dem Gebiet des Testens mechatronischer Systeme und der Umsetzung von XiL-Testumgebungen einbrachte. Die Arbeiten fanden anfangs in der Arbeitsgruppe AG1 “Orchestrierung der Testinfrastruktur – Durchstich TP4” mit Beteiligung der Projektpartner Valeo, BMW, Bosch, FhG, FZI, ZF und Ford statt. Im Rahmen der Arbeitsgruppe erfolgte die Harmonisierung, Detaillierung und Ausgestaltung des Prozessschrittes “Testorchestrierung”, der zuvor im Rahmen der TP4 Arbeitsgruppe AP1 “AG1 Schnittstelle TP4-7" erarbeitet wurde. Die spezifischen Ziele des LBF (Ergebnis E7.2a) orientiere sich an der geplanten Umsetzung einer XiL-Umgebung (TP7.3) zur Nachbildung der Vibrationsanregung eines optischen Sensorsystems. Die Methodenentwicklung und Konzeption von Testinfrastrukturen umfasst dabei die Ableitung technischer Anforderungen an Testeinrichtungen sowie mögliche Gütekriterien. Auch muss eine Abschätzung und Verteilung von Testaufwänden auf unterschiedlichen Testinstanzen ermöglicht werden. Die Erarbeitung genannten Fragestellungen wurden zur Ableitung erster technischer Anforderungen an eine XiL-Umgebung (TP7.3) genutzt. Im frühen Verlauf des TPs fanden ebenfalls Gespräche mit den Partnern FZI, dSPACE und Valeo statt, um mögliche Aktivitäten zur Umsetzung einer XiL-Umgebung zu parallelisieren. Im weiteren Verlauf der Arbeiten stellte das LBF exemplarische Testdurchführungen mit einem mechanischen Hardware-in-the-Loop Prüfstand vor.

Im Zuge der Beteiligung an der Arbeitsgruppe 2 „Einbindung neuer Testmittel in die Validierung“ (AG2) und der Fokussierung der Aufgaben des AP7 mit Hinblick auf das Halbzeitevent erfolgte im Juli 2021 eine Neuausrichtung der Zielsetzungen der AG2 zur Ermittlung von technischen Testanforderungen in einem Bottom-Up Prozess. Im Rahmen der wöchentlichen Regelmeetings der AG2 hat das Fraunhofer LBF eine exemplarische Testfallbeschreibung bereitgestellt, anhand derer wesentliche Teilschritte der Ermittlung und Beschreibung von technischen Testanforderungen gemeinschaftlich mit den Projektpartnern diskutiert und ermittelt wurden. Das bereitgestellte Beispiel einer „Multiaxialen Testumgebung zur Prüfung hochdynamischer Komponenten“[11] betrachtet hierbei ähnliche Gütekriterien an ein Testmittel, wie im Bereich der Schwingungsprüfung mittels x-in-the-Loop (vgl. Abschnitt AP7.3). Das betrachtete Beispiel zu Ermittlung technischer Testanforderungen soll im Folgenden kurz beschrieben werden.

Bei der multiaxialen Prüfung schwingungsbelasteter Steuergeräte (vgl. Abbildung 30) werden – zuvor im Fahrbetrieb an der Einbauposition des Steuergeräts – gemessene Vibrationen reproduzierbar im Labor/Prüffeld „nachgefahren“. Ziel der Prüfungen ist die Optimierung der Schwingungseigenschaften der Leiterplatte mit integrierter MEMS-Beschleunigungssensorik.

[11] "Multiaxiale Testumgebung zur Prüfung hochdynamischer belasteter mechatronischer Komponenten" (Vrbata, J. et. al. DVM-Workshop "Zuverlässigkeit mechatronischer und adaptronischer Systeme").

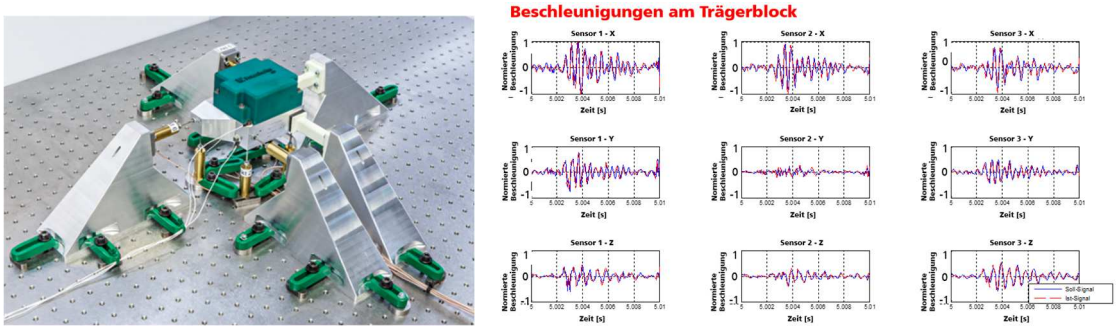


Abbildung 30: Schwingungsprüfstand für multiaxiale Schwingungstests von E/E-Komponenten

Bei der multiaxialen Prüfung schwingungsbelasteter Steuergeräte (vgl. Abbildung 30) werden – zuvor im Fahrbetrieb an der Einbauposition des Steuergeräts – gemessene Vibrationen reproduzierbar im Labor/Prüffeld „nachgefahren“. Ziel der Prüfungen ist die Optimierung der Schwingungseigenschaften der Leiterplatte mit integrierter MEMS-Beschleunigungssensorik.

Der durchlaufene Bottom-Up Prozess zur Testfallbeschreibung, der Ableitung von Testspezifikationen, der Beschreibung von technischen Anforderungen und der Ableitung einer funktionalen Testanforderung sind in Tabelle 1 dargestellt.

Tabelle 1: Bottom-Up Prozess der exemplarischen Testfallbeschreibung.

Begriff	**Beschreibung**
Testfall (Schritt 1 aus Bottom-Up)	**Device under Test** - Steuergerät mit integrierter Beschleunigungsmessung mittels MEMS-Sensoren **Testinstanz** - xIL-Prüfstand / Schwingungsprüfstand **Testmittel** - Multiaxialer, hochdynamischer Schwingungsprüfstand **Testbeschreibung** - Montage des Steuergeräts im Prüfstand - Charakterisierung des dynamischen Verhaltens des Prüfstands mit angeschlossenem Steuergerät - Optimierung der Stellgrößen und Prüfstandsregelparameter - Durchlauf eines Szenarios - Auswertung der Ergebnisse; Erstellung von Plots zur Darstellung **Szenarien** - Harmonische Anregung bei einer festgelegten Frequenz in eine definierte Raumrichtung - Harmonische Anregung mit kontinuierlich steigender Frequenz (Sweep) - Nachbildung der Schwingungsmessdaten am Installationsort des Steuergeräts aus Fahrbetriebsmessung (Manöver X,Y,Z) **Key Performance Indicators** - Nachbildungsgüte der Schwingungssignaturen: Maximale Abweichung des Frequenzgangs (Sollsignal vs. Ist-Signal) in einem definierten Frequenzbereich (f_{min} .. f_{max})

Begriff	Beschreibung
Testspezifikation (Schritt 2 aus Bottom-Up)	**Schwingungsanregung** eines Steuergeräts der neuen Generation mit Schwingungssignaturen, die im Fahrbetrieb mit der vorangegangenen Steuergerätegeneration erfasst wurden: - Technische Informationen zum Prüfling (Abmessungen, Gewicht und Montagepunkte des Prüflings) - Schwingungssignaturen die nachgebildet werden sollen (Manöver) **Gütemaß** (durch was äußert sich das unkritische strukturdynamische Verhalten?) - Einfluss von Resonanz/Nullstelle im strukturdyn. Übertragungsverhaltens des Steuergerätes im Messbereich (0..500 Hz) des MEMS-Sensors kleiner als +/- 1 dB
Technische Testanforderung (Schritt 3 aus Bottom-Up)	[beinhalten Testspezifikation] - Abweichungen der Schwingungsanregung des Steuergeräts im Amplitudenspektrum maximal +-5% vom Vorgabewert unterschiedlicher Manöver für jede Frequenzstützstelle im Frequenzbereich von 350..3000 Hz - Abweichungen der Schwingungsanregung des Steuergeräts im Amplitudenspektrum maximal +-10% vom Vorgabewert unterschiedlicher Manöver alle weiteren Frequenzstützstelle im Frequenzbereich von 0..7000 Hz - Nachbildung in allen Raumrichtungen (X,Y,Z sowie rotatorische Freiheitsgrade) simultan und gleichzeitig - Erfassung des strukturdynamischen Übertragungsverhaltens an der Montageposition des MEMS-Sensors
Funktionale Testanforderung (Schritt 4 aus Bottom-Up)	**Nachweis eines unkritischen strukturdynamischen Verhaltens**

Im Zuge der fortlaufenden Bestrebungen zur Vereinheitlichung von Begrifflichkeit, beteiligte sich das Fraunhofer LBF im Rahmen der AG2 darüber hinaus an der Entwicklung eines Formats zur Testfallbeschreibung über verschiedene Testinstanzen. Hierzu wurden die zuvor erarbeiteten Bottom-Up Testbeschreibungen analysiert und eine erste Version der Struktur einer harmonisierten technischen Testbeschreibung erstellt. Neben Metainformationen, die beispielsweise das Testziel beschreiben, beinhaltet die Struktur der technischen Testbeschreibung ebenfalls Erläuterungen zur genutzten Testinfrastruktur (Testmethode und -instanz), eine Beschreibung der Testsequenz und dem (zeitlichen) Testablauf sowie eine konkrete Beschreibung der Testfälle.

Im weiteren Verlauf der Projektbearbeitung und der Ergebnisbereitstellung für das Deliverable D07 begann das Fraunhofer LBF mit der Ausgestaltung exemplarischer Testbeschreibungen für zwei Testfälle, die sich mit der Untersuchung des Degradationsverhaltens von optischen Sensorelementen beschäftigen. In beiden Fällen soll der Einfluss von Vibrationen auf ein Kamerasystem mittels einer XiL-Methode untersucht werden. Der erste Testfall dient der Ermittlung von Pixelinformationen eines Kamerasystems, das betriebstypischen Vibrationsbelastungen

ausgesetzt ist. Im zweiten Testfall soll das Degradationsverhalten unter Vibrationsbelastung im Gesamtfahrzeugkontext untersucht werden.

Nach der Neuorganisation der Schnellbootaktivitäten im Nachgang des TP7-Quartalstreffens am 21. September 2022 beteiligte sich das LBF aktiv am neu geschaffenen Schnellboot (B) Testorchestrierung gemeinsam mit den Projektpartnern ZF, Valeo, FZI, ProStep, Bosch und Continental. Die Testorchestrierung (Abbildung 31) ist dabei als ein Baustein und Prozessablaufschritt im V&V Assurance Framework zu verstehen.

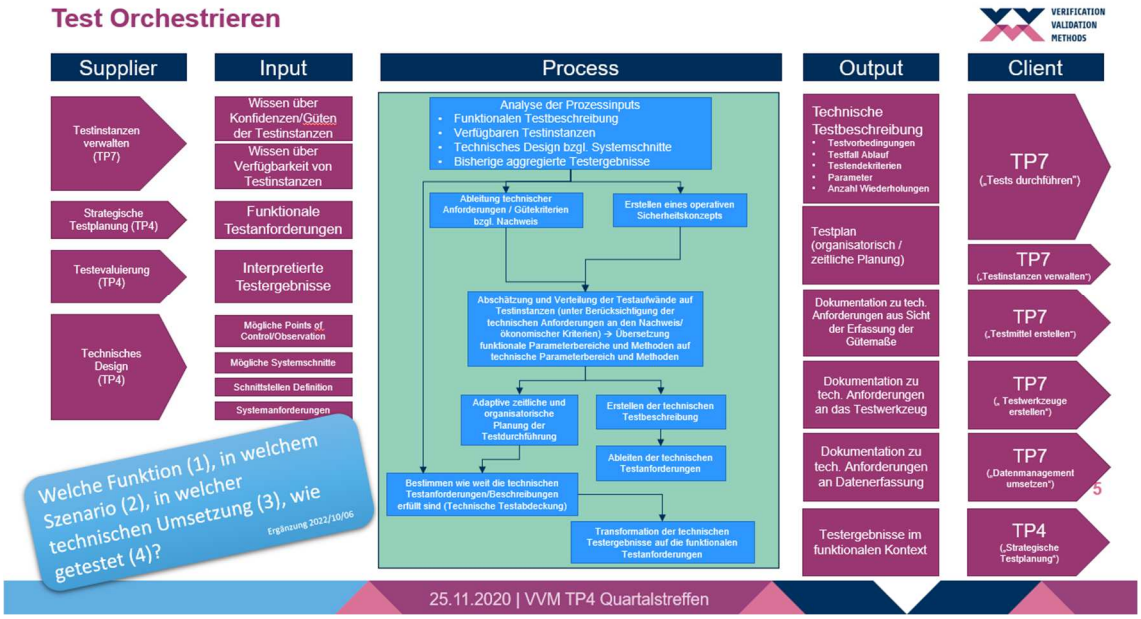


Abbildung 31: Prozessschaubild zur Testorchstrierun

Im weiteren Verlauf erfolgte die Detaillierung und Schnittstellenbeschreibung des Prozessschrittes „Textorchestrierung". Das LBF moderierte dabei die Treffen zur Konkretisierung des Prozessschrittes „Zuordnung". Der Prozessschritt der Zuordnung gewährleistet dabei für eine bereitgestellte Information zur Umgebung (Szenario), das ausgewählte physische Testobjekt und die physischen Zielgrößen unter Berücksichtigung (vorhandener) Testplattformen die Zuordnung einer Testinstanz unter zeitlichen, monetären und qualitativen Anforderungen an den Test (Güten).

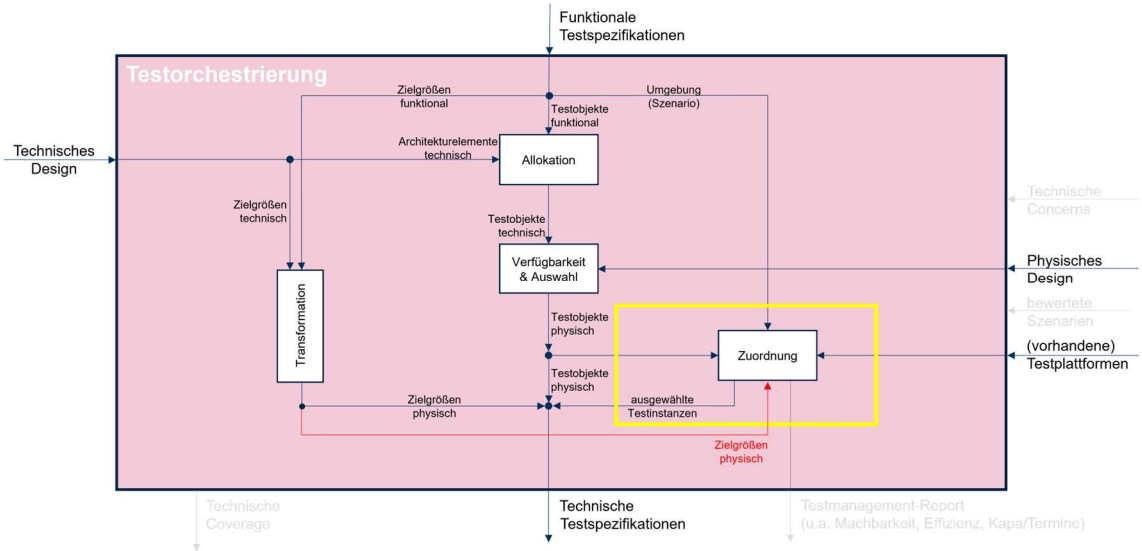


Abbildung 32: Detaillierung der Testorchestrierung mit dem Prozessschritt zur „Zuordnung“ einer Testinstanz.

Tabelle 2 fasst die Eingangsgrößen in den Prozessschritt „Zuordnung“ noch einmal zusammen.

Tabelle 1: Eingangsgrößen des Prozessschritts „Zuordnung“

Eingangsgröße	Beschreibung
Testobjekt (physisch)	○ Informationen zum Testobjekt ○ Technische Schnitte ○ Ggf. adressierte technische Concerns
Zielgröße (physisch)	○ Was soll untersucht werden? (Bsp.: Flankensteilheit BUS-Signal mit def. Güte)
Umgebung (Szenario)	○ Informationen zur ODD, ausgewählten Szenarien und Variationsvorschriften (Parameterräume, Häufigkeiten,…)
(vorhandene) Testplattform	○ Verfügbare Testplattformen ○ Wissen über Fähigkeiten und Güten der Testplattformen und numerischen Modellen für Restsystemsimulationen ○ Ressourcenbedarf (Zeit, Kosten, Infrastruktur, Personal, Energie,…)

Basierend auf den bereitgestellten Eingangsinformationen wurden im Rahmen der gemeinsamen Detaillierung fünf Teilprozessschritte zur Zuordnung definiert: Im **ersten Schritt** erfolgt eine Analyse der Szenarien, den abzudeckenden Parameterräumen und der ODD. Der **zweite Schritt** adressiert die Vorauswahl von Testplattformen mit dem Ziel prinzipiell geeignete Testplattformen auszuwählen, die in der Lage sind das Szenario auszuführen (bspw.: Beurteilung hinsichtlich Abdeckung der Parameterräume, Risiko bei der Durchführung. Im **dritten Schritt** erfolgt die Sicherstellung der Integrierbarkeit des physischen Testobjekts für die betrachteten Testplattformen. Sind die ausgewählten Testplattformen in der Lage das Szenario durchzuführen und kann das physische Testobjekt in die jeweiligen Testplattformen integriert werden, so erfolgt im **vierten Schritt** die Ermittlung der erreichbaren Güten je instanziierter Testplattform und eine Auswahl der Testplattformen, die die geforderte (Mindest-)Güte erreichen können. Für diese Testplattformen erfolgt ferner eine Abschätzung notwendiger Ressourcen zur Durchführung des Tests. Da zu erwarten ist, dass die in den Dimensionen erreichbare Güte und Ressourcenbedarf bewerteten Testplattformen ein pareto-optimales Verhalten aufweisen, sieht der **fünfte Schritt** die abschließende Auswahl einer instanziierten Testplattform vor.

Ergebnis des Teilprozessschrittes „Zuordnung“ ist die Auswahl einer Testplattform unter Berücksichtigung von physischen Zielgrößen, physischem Testobjekt und Umgebung. Zudem können zusätzliche Informationen zur Instanziierung (bspw.: ausgewählte numerische Modelle)

bereitgestellt werden. Teilergebnisse des Teilprozessdurchlaufs können ebenfalls an übergeordnete Prozessschritte (Testmanagement) zurückgespielt werden. Hierzu zählt ebenfalls die Mitteilung, dass – unter den gegeben Eingangsinformationen und den vorhandenen Testplattformen – ggf. keine Zuordnung möglich war.

1.1.4.3 AP7.3 Exemplarische Referenzumsetzung

Im Zuge von *TP7.3 Exemplarische Referenzumsetzung* leistete das LBF mit der Umsetzung einer XiL-Testumgebung einen Beitrag zur praktischen Umsetzung eines Testkonzeptes aus TP7.2.

Zu Beginn beteiligte sich das LBF an einer Arbeitsgruppe zur Erarbeitung einer Co-Simulationsarchitektur für eine Closed-Loop-Simulation mit den Partnern AVL, dSPACE und FZI. Hierbei waren geeignete Modelle zur Simulation von Vibrationsanregungen an verschiedenen Sensormontagepositionen im Fahrzeug Gegenstand der Beiträge des LBF, wobei auf Fahrzeugmodelle des Schwesterprojektes SetLevel aufgegriffen wurden. Das für eine Co-Simulation und/oder XiL-Restsystemsimulation verwendete Modell soll dabei das reduzierte Modell eines Fahrzeugchassis, ein dynamisches Reifenmodell sowie die Möglichkeiten zur Simulation einer unebenen Fahrbahn beinhalten. Das Fraunhofer LBF initiierte hierzu eine Abstimmung mit den Ansprechpartnern von SetLevel mit dem Ziel, Möglichkeiten einer konsistenten Co-Simulationsumgebung abzustimmen und ein Modellaustauschformat – das eine Nutzung im xIL-Prüfstand zulässt – zu vereinbaren. Modellaustauschformate von hoher Relevanz sind dabei ordinäre, signalflussbasierte Beschreibungen in Matlab/Simulink, Functional Mock-up Units (FMU), sowie C-Code oder pre-kompilierte Bibliotheken. Basierend auf den Anforderungen an die Co-Simulation und Restsystemsimulation im Rahmen der xIL-Prüfung wird die Dynamik als einfache Starrkörperbewegung des Fahrzeugs nachgebildet. Niederfrequente Schwingungen können dabei aufgrund der Wechselwirkungen der anderen Bestandteile des Modells (insbesondere Achse, Dämpfer, Reifen, Antriebsstrang) reproduziert werden. Für die Nachbildung dynamischer Schwingungen, die sich aus der Strukturdynamik der Fahrzeugkarosserie (bspw. durch mechanische Resonanzen) ergeben, wurde eine Schnittstelle zu einem reduzierten Finite-Elemente-Schwingungsmodell vorgesehen. Die Schnittstellen des Fahrdynamik- und des reduzierten Finite-Elemente-Modells sind dabei die wirkenden Kräfte und Momente an den karosserieseitigen Fahrwerksanbindungen.

Im Rahmen der Aktivitäten der CO-Simulationsarbeitsgruppe hat das Fraunhofer LBF ebenfalls die Möglichkeiten zur Integration von OpenCGR-Straßenmodellen[12] untersucht. Die bereitgestellten Anwendungsbeispiele stellen dabei Straßeninformationen (Fahrbahninformationen, Neigung, Höhe) in hoher Auflösung bereit. Ein Zugriff auf die Straßeninformationen ist in OpenCRG sowohl über ein globales Koordinatensystem als auch über ein – der Straße mitgeführtem – Koordinatensystem möglich. Das betrachtete Beispiel „Country Road“, was in Abbildung 33 visualisiert ist, stellt dabei eine Landstraße mit 568 m Länge und einer Straßenbreite von 3,7 m zur Verfügung. Insgesamt werden ca. 21 Mio. Datenpunkte für die Höheninformation der Straße im Single-Precision-Datenformat zur Verfügung gestellt.

[12] https://www.asam.net/standards/detail/opencrg/

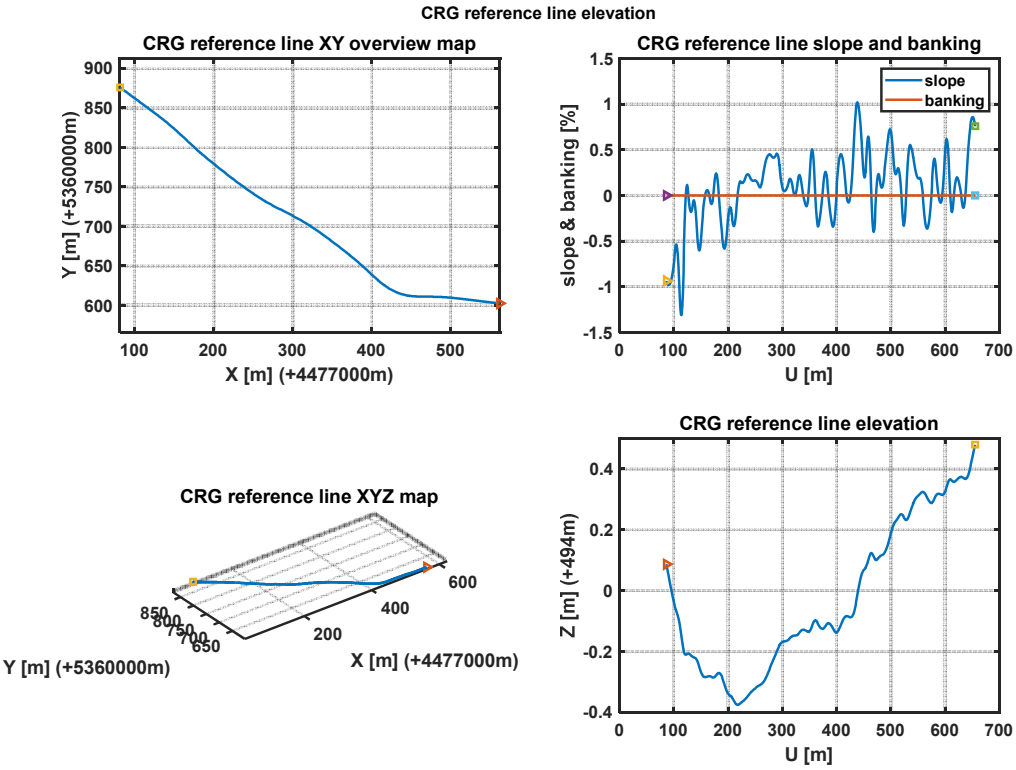


Abbildung 33: Importiertes OpenCRG-Straßenprofil („Country Road“)

Basierend auf den importierten Höheninformationen wurde eine vereinfachte Schwingungssimulation (Viertelfahrzeug) umgesetzt, um die spektralen Anteile und damit die Bandbreite der im Straßenprofil enthaltenen Störungen zu untersuchen. Abbildung 34 zeigt die Ergebnisse der Voruntersuchung für eine Fahrt des Viertelfahrzeugs mit einer konstanten Geschwindigkeit von 30 km/h. Im Beschleunigungsspektrum können Beschleunigungen bis zu einem Frequenzbereich von etwa 160 Hz beobachtet werden.

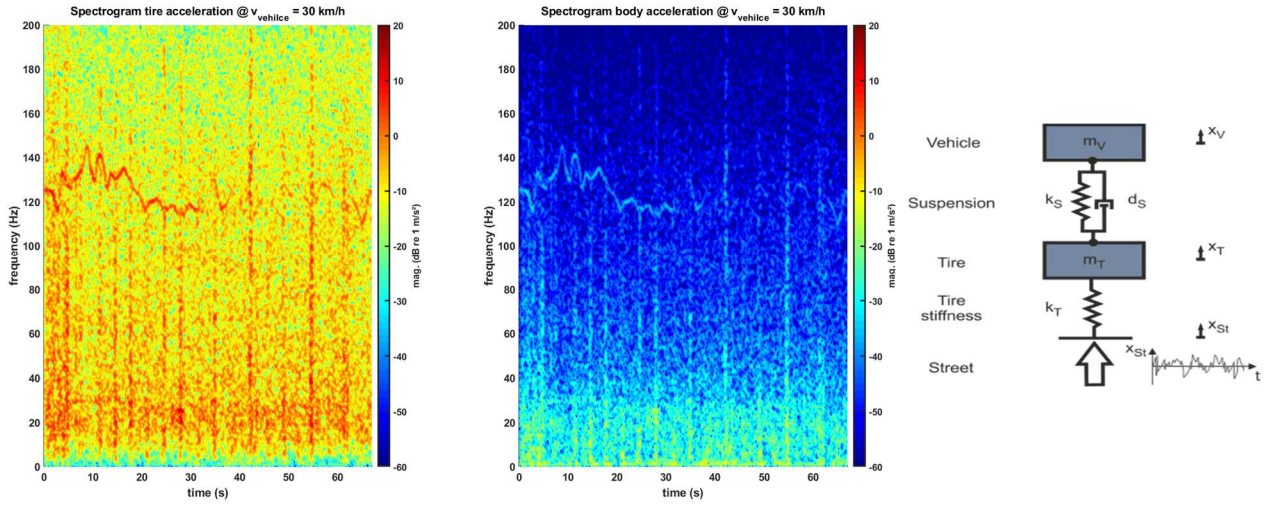


Abbildung 34: Simulationsergebnisse der resultierenden Fahrzeugschwingungen und vereinfachtes Viertelfahrzeugmodell

Ein dynamisches Fahrzeugmodell zur Simulation von Fahrzeugvibrationen sowie ein OpenCRG-Straßenmodell stellte das LBF den Partnern von TP7.3 als Functional Mock-up Unit (FMU) zur Verfügung.

Nach dem Abschluss der Arbeiten zur Co-Simulation fanden gemeinsame Gespräche mit den Partnern FZI und dSPACE zur Konzeptionierung und Umsetzung einer XiL-Umgebung statt, die die Analyse von Vibrationsbelastungen auf optische Sensorsysteme ermöglicht. Hierbei stellt das Kamerasystem das System-under-Test dar. Ein dynamisches Fahrzeugmodell aus SetLevel modelliert das Schwingungsverhalten an veränderbaren Montagepositionen im Fahrzeug. Die berechneten Fußpunktbewegungen des Montagepunktes der Kamera werden als Soll-Signal an ein mechanische Hardware-in-the-Loop-Schnittstelle übermittelt, die das in der Echtzeitsimulation berechnete Schwingungsverhalten auf das reale Kamerasystem aufprägt. Das Fahrzeugmodell ist dabei zudem mit einer Umgebungssimulation verknüpft, die ein Rendering der Szene berechnet und auf einem Bildschirm darstellt. Die – mit den Fahrzeugschwingen belastete – Kamera erfasst das Bild der Szene und stellt die Pixelinformationen zur Verfügung. Eine Bewertung der Sensitivität des Kamerasystems mit Hinblick auf die Schwingungsanregung am Montagepunkt ist das Ergebnis der Untersuchungen. Hierbei können die aufgenommen Pixelinformationen der Kamera direkt bewertet oder – sofern ein Klassifikator bereitsteht – die Erkennungsgüte der in der Szene vorhanden Objekte ermittelt werden.

Im Zuge der Umsetzungen des Konzeptes stellte das LBF ein erstes Mock-up des XiL-Schwingungsprüfstandes im Rahmen des ITS World Congress in Hamburg vor. Abbildung 35 zeigt den umgesetzten Demonstrator. Hierbei integriert der Demonstrator eine Echtzeitsimulation des Schwingungsverhaltens des Fahrzeugs und ein Rendering der Umgebung. Ein mechanische Hardware-in-the-Loop-System prägt die berechneten Fußpunktbewegungen in das Kamerasystem ein. Zur Umsetzung des Demonstrators wurde im ersten Schritt eine konventionelle WebCam eingesetzt. Die – durch die Schwingungsanregung verzerrten – Kamerabilder werden auf den großen Monitor übertragen und zeigen vereinfacht die Empfindlichkeit des Kamerasystems gegenüber den herrschenden Schwingungen am Montagepunkt des Kamerasystems auf.

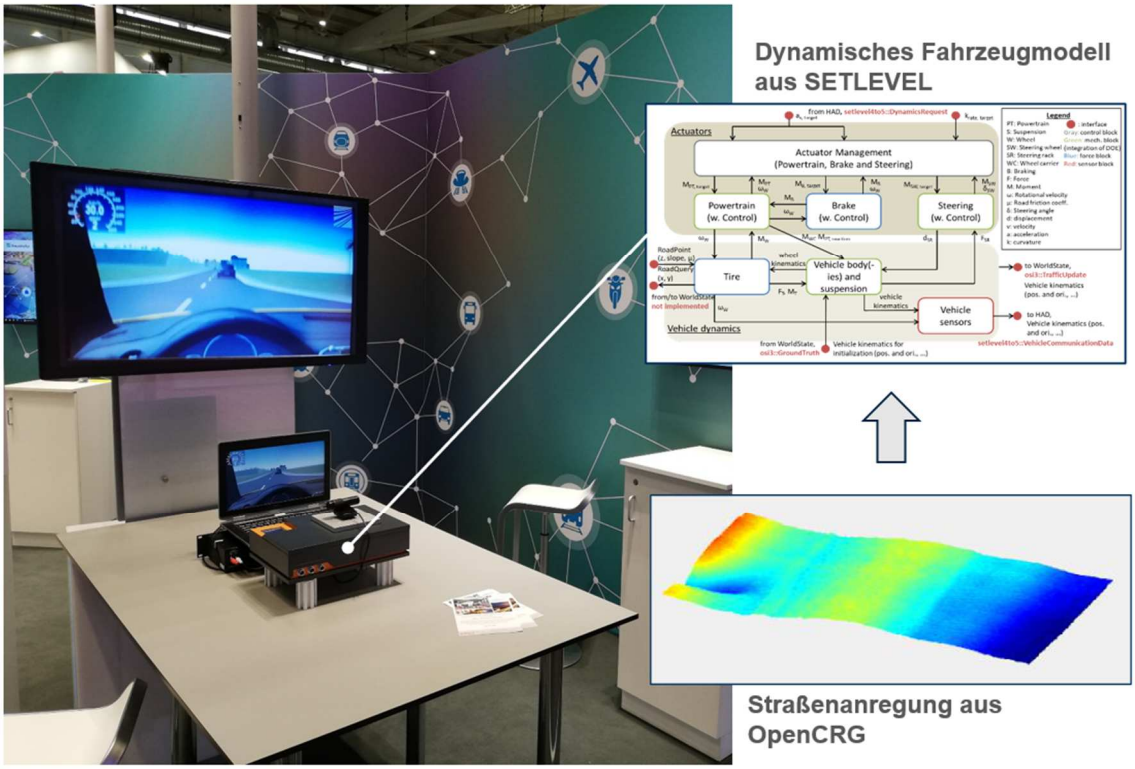


Abbildung 35: Mock-up der x-in-the-Loop Schwingungsumgebung.

Abbildung 36: XiL-Experte Jonathan Millitzer (Fraunhofer LBF) im Austausch mit Fraunhofer-Präsident Prof. Neugebauer und Bernd Lange (Abgeordneter des Europäischen Parlaments).

Das Mock-Up des XiL-Testkonzepts stellte das Fraunhofer LBF darüber hinaus öffentlichkeitswirksam auf der Hannovermesse vor. Beim Vorstandsrundgang konnten sich Prof. Neugebauer (ehm. Präsident der Fraunhofer-Gesellschaft) und Bernd Lange (Abgeordneter des Europäischen Parlaments) unmittelbar über die Herausforderungen und Zielsetzungen des Projektes informieren (vgl. Abbildung 36).

Im Zug der weiteren Arbeiten wurden manipulierbarer Eigenschaften und Randbedingungen der XiL-Umgebung ermittelt, die – aus Sicht der Schwingungstechnik – einen parasitären Einfluss auf das aufgenommene Kamerabild haben können. Abbildung 37 fasst diese Eigenschaften in den Dimensionen Anregung (Excitation), Szenario und dem eingesetzten virtuellen Fahrzeugmodell (virtual vehicle model) zusammen.

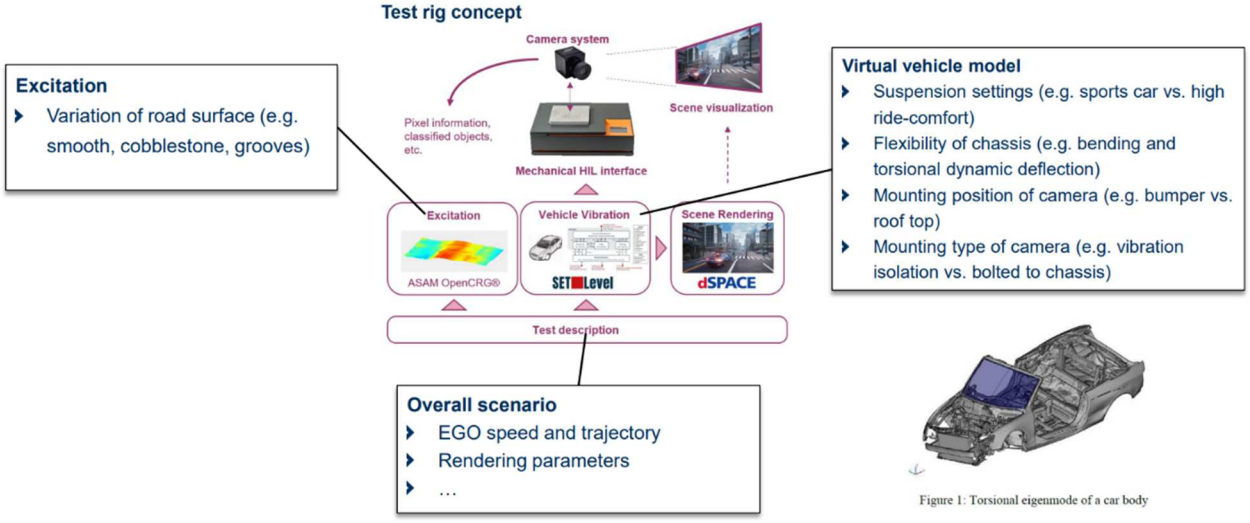


Abbildung 37: Veränderbare Eigenschaften und Randbedingungen, die aus Sicht der Schwingungstechnik parasitäre Effekte auf das aufgenommene Kamerabild haben können.

In Anlehnung an den ASAM Test Specification Study Group Report[13] erarbeitete das LBF ebenfalls mögliche Storylines zur Darstellung und Verortung der XiL-Testumgebung im Rahmen des VVM-Abschlussevents zur Diskussion. Basierend auf den Ergebnissen der ASAM-Arbeitsgruppe lässt sich die praktische Umsetzung der XiL-Testumgebung hinsichtlich der Testumgebung in den sowohl im Bereich *Hardware Re-Processing* als auch im Bereich *Closed-Loop HIL* verorten. Im Bereich der Testmethoden können – sofern validierbare Anforderungen hinsichtlich der tolerierbaren Schwingungsbelastung definiert werden können – Tests zur Validierung von Anforderungen durchgeführt werden. Auch bietet die XiL-Testumgebung die Möglichkeit eines Fault-Injection-Tests, wenn Vibrationen als parasitärer Effekt verstanden werden. In beiden Fällen stellt die xIL-Testumgebung ein Testmittel bereit, mit dem sich szenarien-basierte Testabläufe durchführen lassen.

Um synergetische Effekte bei einer partnerübergreifenden Umsetzung von Testumgebungen zu eruieren, initiierte das LBF einen eintägigen Workshop beim Partner FZI in Karlsruhe. Beim Vorortttermin wurde eine mögliche Integration der xIL-Testumgebung zur Nachbildung von Vibrationen in die vorhandenen Kamerabox des FZI (Abbildung 38) diskutiert. Sowohl FZI als auch LBF bewerteten die Synergieeffekte sehr positiv, sodass die für konstruktive Ausgestaltung und Umsetzung des mehraxialen Schwingerregers der XiL-Testumgebung nun vorgesehen war, dass dieser in die Kamerabox des FZI integriert werden kann. Die weiteren Arbeiten des LBF fokussierten die praktische Umsetzung einer exemplarischen XiL-Umgebung für den Text eines Kamerasystems unter Vibrationsbelastung.Für die Umsetzung wird eine Einrichtung zur Schwingungserregung einer Kamera in eine bestehende Kamerabox des Partners FZI integriert (siehe Abbildung 38, links). Hierbei filmt eine Kamera das Rendering des Verkehrsraums (FZISim) ab. Die aufgenommene Bildfolge wird im Nachgang zur Perzeption (z.B. Erkennung von Fußgängern) genutzt. Eine Schwingungsanregung der Kamera wird über eine Parallelkinematik mit drei vertikal wirkenden Tauchspulenaktoren gewährleistet. Durch eine Rücktransformation der Bewegungszielgrößen am Kameramontagepunkt werden die Steuersignal der einzelnen Tauchspulenaktoren berechnet.

[13] ASAM Test Specification Study Group Report 2022 (2022): Evolving Landscapes of Collaborative Testing for ADAS & AD. https://www.asam.net/project-detail/test-specification/, Letzter Zugriff: 28.11.2022.

Abbildung 38 (rechts) zeigt die entwickelte Parallelkinematik, Bild 39 das Koordinatensytem der Parallelkinematik.

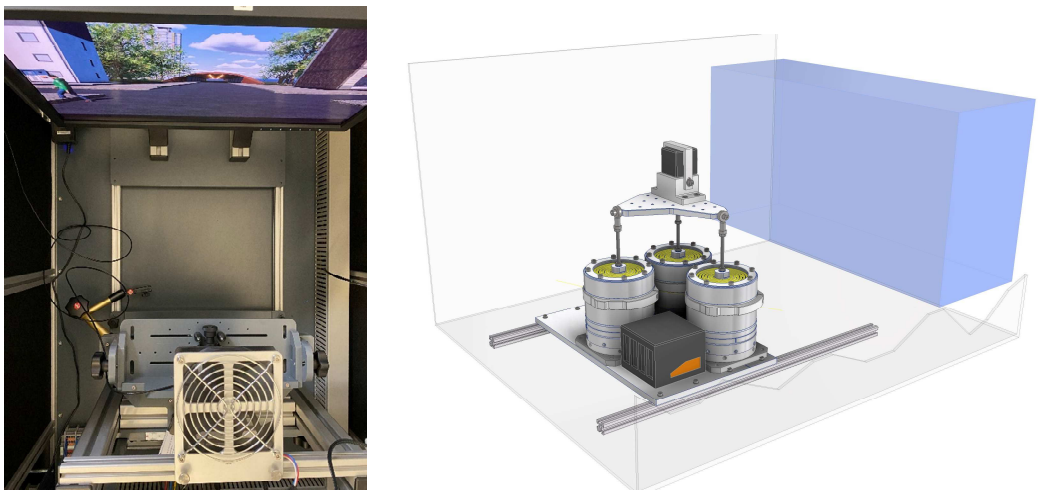


Abbildung 38: Kamerabox des Partners FZI (links) und entwickelte Parallelkinematik mit Kameraaufnahme (rechts).

Basierend auf den simulativen Voruntersuchungen und praktischen Überlegungen ist die Parallelkinematik in der Lage eine dynamische Vertikalbewegung (ca. ± 10 mm) sowie eine dynamische Roll- und Nickbewegung (ca. ± 5 °) simultan nachzubilden. Die Tauchspulenantriebe stellen hierbei kontinuierliche Kräfte von jeweils 90 N und Spitzenkräfte von jeweils 315 N bereit. Eine Vorgabe von Horizontalhub, Roll- und Nickwinkel ist bis zu einer maximalen Frequenz von etwa 200 Hz möglich.

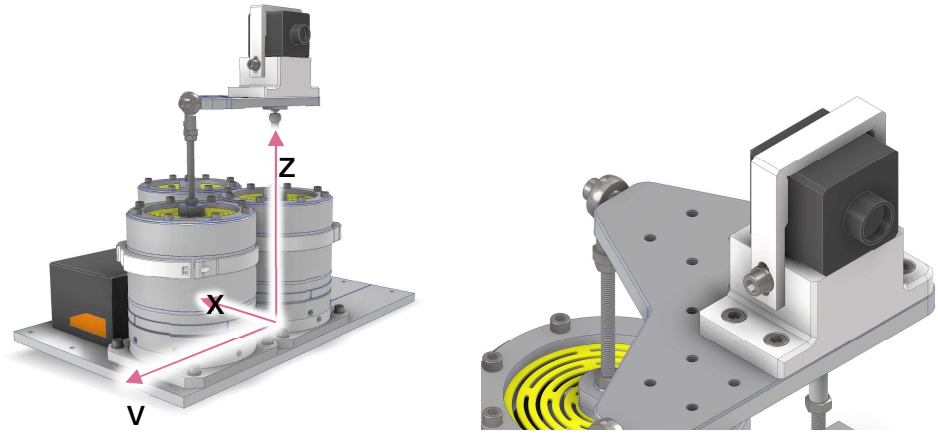


Abbildung 39: Koordinatensystem der Parallelkinematik zur Schwingungsanregung (links) und Detaildarstellung der Kameraaufnahme (rechts).

Neben der Auswahl geeigneter Tauchspulenaktoren und der konstruktiven Ausgestaltung der Parallelkinematik wurden ebenfalls geeignete Leistungsverstärker zur Steuerung der Parallelkinematik ausgewählt. Aufgrund der kleinen Baugröße und der geringen Verlustleistung fiel die Wahl hierbei auf einen schaltenden Klasse-D-Verstärker. Bei der Realisierung von drei Vollbrückenverstärkern zur Ansteuerung der Tauchspulenaktoren kommen Halbbrücken-ICs der Baureihe BTN8982TA zum Einsatz. Die nominelle Leistung der Vollbrückenverstärker beträgt etwa 250 W. Die Auswahl der Leistungsverstärker wurde durch eine vereinfachte Tauchspulenaktorsimulation unterstützt. Abbildung 40 zeigt die sich ergebenden Weg-, Beschleunigungs- und Stromamplituden eines Aktors bei harmonischer Ansteuerung mit

Spannungssignal mit 18 V Amplitude. Da die Tauchspulenaktoren konstruktionsbedingt durch eine vertikal wirkendes Steifigkeitselement gehalten werden, ergibt sich eine mechanische Eigenfrequenz (bei ca. 20 Hz), die bedingt durch die hohe Gegeninduktion des Tauchspulenaktors, stark gedämpft erscheint. Im betrachteten Beispiel beträgt der maximale Hub etwa 12 mm bei einer Frequenz von 17 Hz. Bedingt durch die Masseneffekte des Aktors können bei einer Frequenz von 100 Hz noch etwa 400 µm Hub erreicht werden. Das erreichbare Niveau der Beschleunigungsamplituden beträgt zwischen 70 - 110 m/s² im Frequenzbereich zwischen 17..100 Hz.

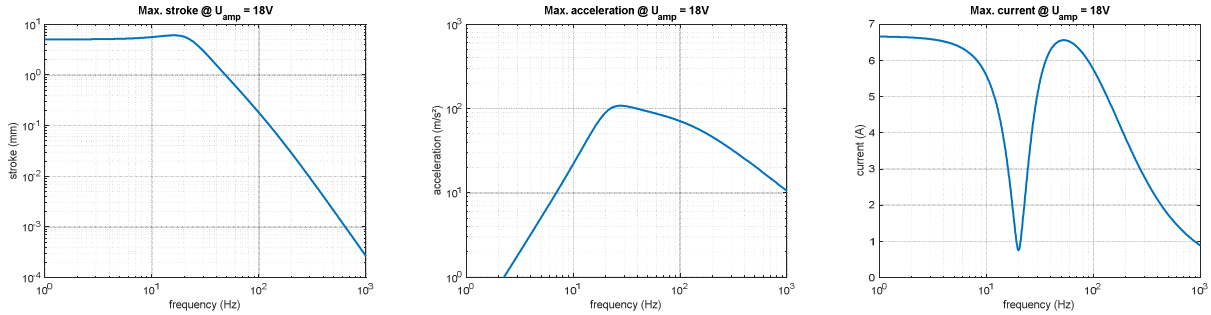


Abbildung 40: Sich einstellende Weg- (links), Beschleunigungs- (Mitte) und Stromamplitude (rechts) eines Tauchspulenaktors bei Ansteuerung mit einem harmonischen Spannungssignal mit 18 V Amplitude.

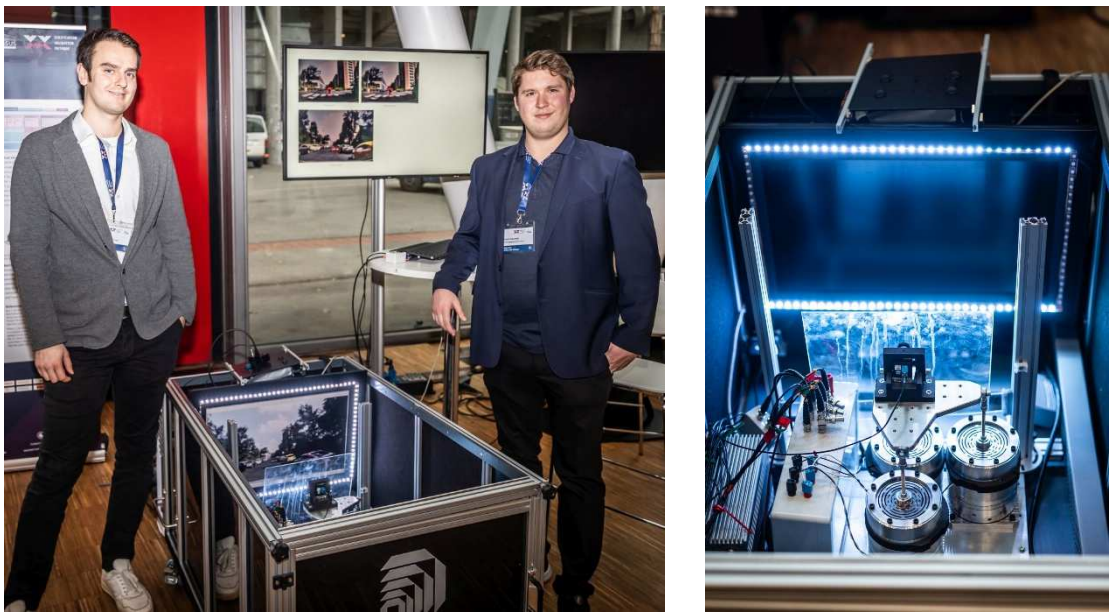


Abbildung 41:Vorstellung der XiL-Testumgebung auf dem VVM-Abschlussevent.

Nach erfolgreicher Inbetriebnahme der XiL-Umgebung gemeinsam mit dem Partner FZI wurde das Testkonzept auf dem VVM-Abschlussevent vorgestellt (Abbildung 41). Hierbei können – basierend auf der Prüfstandsteuerung des FZI – unterschiedliche Fahrszenarien mit und ohne Vibrationsbelastung des Kamerasystems aufgenommen werden. Eine aufgenommene Kamerabildsequenz wird mit automatisiert mit einer Ground-Truth-Objektliste verglichen. Treten Abweichungen zwischen der Ground-Trouth-Objektliste und der durch die Kamera mit Objektklassifizierung gewonnenen Objektliste auf, werden die Abweichungen automatisiert aufgelistet.

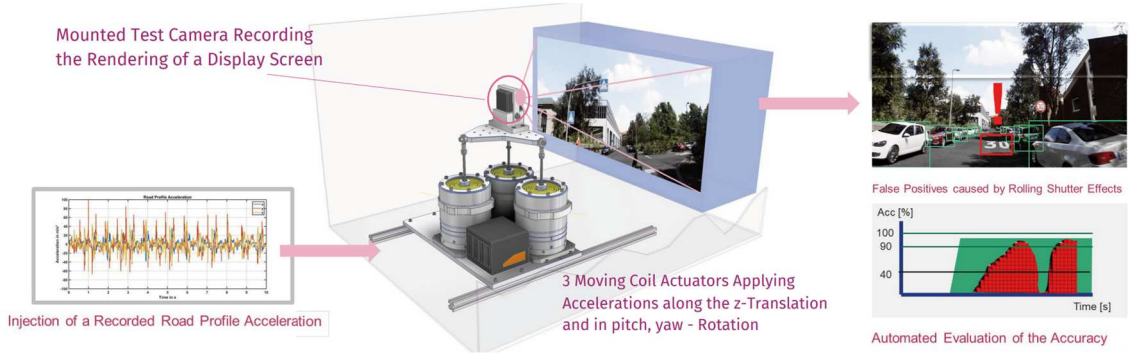


Abbildung 42: Exemplarische Ergebnisse der Untersuchungen mit der XiL-Umgebung.

Abbildung 42 zeigt ein exemplarisches Ergebnis der Untersuchungen. Durch die Erregung der Kamera mit Frequenzen nahe der Bildfolgefrequenz entsteht ein merklicher Rolling-Shutter-Effekt, der beispielsweise dazu führt dass eine Straßenmarkierung fälschlicherweise als stillstehendes Fahrzeug klassifiziert wird.

1.2 Die wichtigsten Positionen des Zahlenmäßigen Nachweises

Die Personalmittel des LBF wurden der Planung entsprechend eingesetzt. Wie zuvor beschrieben, wurden Reisemittel zur Abdeckung der Mehraufwände bzgl. der kommissarischen AP-Leitungen umgewidmet. Die sonstigen unmittelbaren Kosten waren im Wesentlichen den Unteraufträgen für das Management durch EICT bestimmt und auch verausgabt worden.

Ein wesentlicher Posten der Materialkosten war die Umsetzung einer XiL-Testumgebung für den Robustheitstest eines optischen Kamerasystems mit Objekterkennung unter mehraxialer Vibrationsbelastung.

Die Positionen der geplanten Personalmittel für das IESE wurden im Rahmen der aktualisierten Planung eingesetzt. Das eingesetzte Personal war in der erfolgten Einsetzung im Projekt zu Erfüllung der wesentlichen Aufgaben erforderlich, wie

TP3 (~1/3 des IESE-Personalbudgets)

- Erarbeitung der Methode zur nachverfolgbaren modellbasierten Sollverhaltensspezifikation
- Technische Implementierung der Methode mit „Digital Dependability Identitities“

TP4 (~2/3 des IESE-Personalbudgets)

- Erarbeitung der modellbasierten Methode zur Sicherheitsanalyse probFMEA/CFT
- Technische Implementierung der probFMEA/CFT Methode in safeTbox und Digital Dependability Identities
- Koordinierung und Leitung der Arbeiten in Core03 zur Erzeugung des VVM Safety Assurance Frameworks und der projektübergreifenden Sicherheitsargumentation
- Modellierung des VVM Sicherheitsnachweises in der Goal Structuring Notation

Studentische Hilfskräfte wurde insbesondere zur Unterstützung der technischen Implementierung genutzt. Die während Covid nicht angetretenen Reisen von LBF und IESE wurden zugunsten der Priorität auf der Erzeugung der Sicherheitsargumentation in TP4 in Personalbudget umgewidmet.

Das Reisebudget wurde einerseits für Arbeitsworkshops im Rahmen der Projektarbeit verwendet, andererseits zur internationalen Dissemination der Projektergebnisse, z.B. die Reisen auf die TRB ARTS Konferenz in San Francisco sowie die Teilnahme am SIP-ADUS Symposium in Tokyo.

Das Fraunhofer IVI verwendete die Personalkosten für nachfolgende Tätigkeiten:

- Datenauswertung der polizeilichen Unfalldatenbank und Analysezusammenführung mit GIDAS Unfalldatenanalyse zur Definition der Messstellen
- AIMATS Erhebung an den Messstellen (Genehmigung, Installation, Wartung, Deinstallation)
- Verbesserung der Algorithmik zur Auswertung des Videomaterials
- Auswertung der AIMATS Messungen und Aufbereitung / Upload der Ergebnisse für das VVM-Konsortium
- Dokumentation.

Die angegebenen Dachkosten wurden für die behördliche Genehmigung der Erhebung durch die Stadt Dresden aufgewendet.

Die ursprünglich geplanten Reisekosten des IVI von 4.500€ wurden auf Grund der Corona Beschränkungen nicht vollständig verwendet und für die weitere Optimierung des Auswertealgorithmus in Personalkosten umgewandelt.

1.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Fraunhofer leistete im Rahmen des Projekts essenzielle Beiträge zur Entwicklung und Validierung von Methoden zur Sicherstellung der funktionalen Sicherheit und Systemzuverlässigkeit autonomer Fahrzeuge. Die geleistete Arbeit war notwendig, um den komplexen Anforderungen an die Sicherheit hochautomatisierter Fahrfunktionen gerecht zu werden. Durch die Erweiterung etablierter Safety-Analyse-Methoden wie der Component Fault Tree (CFT) Analyse und der probabilistischen FMEA konnte eine detaillierte und umfassende Sicherheitsbewertung durchgeführt werden. Diese Methoden ermöglichten es, potenzielle Risiken und Unzulänglichkeiten systematisch zu identifizieren und zu bewerten, um geeignete Sicherheitsmaßnahmen zu implementieren und zu verifizieren.

Die Integration dieser Methoden in die Digital Dependability Identity (DDI) schuf eine durchgängige Referenzierbarkeit zwischen Safety- und Entwicklungsartefakten, was die Nachvollziehbarkeit und Konsistenz der Sicherheitsnachweise erheblich verbesserte. Zudem wurden im Rahmen der Arbeitspakete spezifische Testanforderungen und Sicherheitskonzepte entwickelt, die zur Erstellung eines konsolidierten Katalogs von Systemanforderungen führten. Diese Arbeiten waren entscheidend, um eine fundierte Basis für die Verifikation und Validierung der autonomen Fahrfunktionen zu schaffen.

Mit den geleisteten Arbeiten wurden stationäre Verkehrsbeobachtungen für das VVM Konsortium nach AIMATS Methodik zur Verfügung gestellt. Die stationäre Erhebung von Verkehrsszenarien ist

eine wichtige Ergänzung der Szenarienerhebung aus der Fahrzeugperspektive anderer Projektpartner.

Die Arbeiten trugen maßgeblich zur Erreichung der Projektziele bei, indem sie innovative und praxisnahe Lösungen zur Absicherung automatisierter Fahrfunktionen entwickelten. Durch die enge Zusammenarbeit mit Industriepartnern und die Veröffentlichung der Ergebnisse in wissenschaftlichen Beiträgen und auf Fachveranstaltungen wurde zudem die praktische Anwendbarkeit und die Verbreitung der entwickelten Methoden sichergestellt. Die geleistete Arbeit war somit nicht nur notwendig, sondern auch angemessen, um die Sicherheit und Zuverlässigkeit autonomer Fahrzeuge im urbanen Umfeld zu gewährleisten und die gesetzten Projektziele zu erreichen.

1.4 Voraussichtlicher Nutzen, insbesondere der Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Fraunhofer hat im Rahmen des Projekts zahlreiche Verwertungsmaßnahmen ergriffen und plant weitere Schritte zur Verwertung der erzielten Ergebnisse. Bereits jetzt wurden die entwickelten Methoden zur funktionalen Sicherheit und Systemzuverlässigkeit, insbesondere die Erweiterungen der Component Fault Tree (CFT) Analyse und der probabilistischen FMEA, in das Tool SafeTbox implementiert. Diese Implementierung ermöglicht eine praxisnahe Anwendung und wird in weiteren Forschungs- und Industrieprojekten genutzt, um die Sicherheit autonomer Fahrzeuge zu gewährleisten.

Darüber hinaus wurden und werden die Ergebnisse in wissenschaftlichen Publikationen veröffentlicht und auf verschiedenen Fachveranstaltungen präsentiert. Dies fördert die Verbreitung und Anwendung der Methoden in der Forschungsgemeinschaft und der Industrie. Die aktive Teilnahme an internationalen Symposien und Workshops trägt zudem zur Harmonisierung von Standards bei und unterstützt die internationale Zusammenarbeit.

Zukünftige Verwertungspläne umfassen die Integration der entwickelten Ansätze in Normungsgremien und Standardisierungsvorhaben, um die Erkenntnisse und Methoden aus dem Projekt in zukünftige Standards einfließen zu lassen. Insbesondere wird der Transfer der Ergebnisse rund um die Safety-Argumentation hochautomatisierter Systeme in nationale und internationale Gremien, wie DKE/AK 801.0.8 und ISO/TC 22/SC 32/WG 13, angestrebt.

Zudem plant das Fraunhofer IESE, die entwickelten Methoden und Technologien in weiteren Forschungsprojekten weiterzuentwickeln. Aktuelle laufende Folgeprojekte umfassen das BMBF-Projekt AutoDevSafeOps und das im Juni 2024 abgeschlossene FhG-interne Förderprojekt „Layes of Protection Architectures for Autonomous Systems“ (LOPAAS) zur Erweiterung des Assurance Frameworks und der Sicherheitsargumentation.

Die im Projekt verwendete und weiterentwickelte AIMATS Methode wurde bereits während der Projektlaufzeit in weiteren Projekten des Fraunhofer IVI zur Szenarienerhebung für einen Industriepartner in Frankreich sowie die Erweiterung der Szenariendatenbank TASC RTS in Kooperation mit der VUFO verwendet. Der Einsatz des Systems für weitere Erhebungen ist geplant.

Diese Maßnahmen sichern nicht nur die Verwertung der Projektergebnisse, sondern tragen auch dazu bei, die wissenschaftliche Sichtbarkeit und die internationale Konkurrenzfähigkeit der deutschen Forschungseinrichtungen zu stärken. Durch die enge Vernetzung mit Industriepartnern und die strategische Ausrichtung auf praxisrelevante Anwendungen wird ein signifikanter

wirtschaftlicher Nutzen für die deutsche Industrie im Umfeld sicherheitskritischer hochautomatisierter Fahrsysteme erwartet.

1.5 Veröffentlichungen

1.5.1 Erfolgte Veröffentlichungen

2021

- J. Millitzer, Vorstellung VVM (XiL-Umgebung) auf ITS World Congress 2021
- Jan Reich (Fraunhofer IESE), Roland Galbas, Thomas Kirschbaum, Frank Junker (Robert Bosch GmbH) Thomas Corell, Björn Filzek (Continental Teves AG & Co. oHG): „Herausforderungen und Lösungsansätze für die durchgängige Freigabeargumentation von automatisierten Fahrfunktionen: Erste Ergebnisse aus dem BMWi „V&V Methoden"-Projekt". TÜV Süd safe.tech Tagung 2021 - Funktionale Sicherheit in der Bahntechnik, Automatisierung und Automobiltechnik.
- Rauschenbach, M.; Kupjetz, S.; Wolschke, C.; Braun, T. (2021): Ansatz zur methodischen Analyse und Absicherung des Funktionalkonzepts voll automatisierter Kraftfahrzeuge. In: Technische Zuverlässigkeit 2021: VDI Verlag, 309-XII, https://doi.org/10.51202/9783181023778-309.

2022

- Roland Galbas, Jan Reich, Helmut Schittenhelm & Nicolas Wagener: „Safeguarding Methods for Complex Traffic Scenarios for Approval of Automated Driving Functions". ATZ Worldwide 124, 56–61.
- Hans Nikolaus Beck, Nayel Fabian Salem, Veronica Haber, Matthias Rauschenbach, Jan Reich „Phenomenon-Signal Model: Formalisation, Graph and Application". https://arxiv.org/abs/2207.09996
- Nayel Fabian Salem, Veronica Haber, Matthias Rauschenbach, Marcus Nolte, Jan Reich, Torben Stolte, Robert Graubohm, Markus Maurer. „Ein Beitrag zur durchgängigen, formalen Verhaltensspezifikation automatisierter Straßenfahrzeuge" https://arxiv.org/abs/2209.07204
- Thilo Bein, Heiko Atzrodt, Riccardo Bartolozzi, Simon Kupjetz, Jonathan Millitzer, Jürgen Nuffer, Matthias Rauschenbach, Georg Stoll, Verification and validation of automated driving systems utilizing probabilistic FMEA and simulation approaches, Transportation Research Procedia, 2022, https://doi.org/10.1016/j.trpro.2022.
- Jonathan Millitzer, Vorstellung VVM (XiL-Umgebung) auf der HMI2022
- *Roland Galbas, Jan Reich, et al.: Absicherungsmethoden für komplexe Verkehrsszenarien zur Freigabe automatisierter Fahrfunktionen. Automobiltechnische Zeitung, Springer Verlag*

2023

- M. Rauschenbach, Jürgen Nuffer, Simon Kupjetz: probFMEA - best of two Worlds – Industrie Workshop 2023

- N. F. Salem et al., "Risk Management Core—Toward an Explicit Representation of Risk in Automated Driving," in IEEE Access, vol. 12, pp. 33200-33217, 2024, doi: 10.1109/ACCESS.2024.3372860.
- FISITA 2023; FWC2023-CYB-005; Schreiber, D., Schramm, S.; Saadé, J; Mallada, J.; Monitoring of French intersection traffic – the application of anhanced AIMATS-system
- ADAS Experience 2023; Erbsmehl, C.; Braitlauch, P.; From Real World Scenarios to Real World Testing
- FISITA 2023; FWC2023-CYB-005; Schreiber, D., Schramm, S.; Saadé, J; Mallada, J.; Monitoring of French intersection traffic – the application of anhanced AIMATS-system
- ADAS Experience 2023; Erbsmehl, C.; Braitlauch, P.; From Real World Scenarios to Real World Testing
- Alle Institute/Autoren: Vorstellung der Ergebnisse in Vorträgen und Postern beim Mid-term und Final Event, wo Fraunhofer maßgebende gestalterische Rolle innehatte (u.a. Vorträge Jan Reich und Jürgen Nuffer)

1.5.2 Geplante Veröffentlichungen

- Beitrag bei der Tagung Technische Zuverlässigkeit 2025, thematisch angesiedelt im Bereich „Ableitung von System- und Testanforderungen“, Titel t.b.d.