Absicherung von Systemen für das (hoch)automatisierte Fahren

Matthias Stiller
Corporate Systems & Technologies
Continental Teves AG & Co.oHG
Guerickestr. 7
60488 Frankfurt
matthias.stiller@continental-corporation.com

Abstract: Der Übergang vom assistierten Fahren zum (hoch)automatisierten Fahren stellt eine enorme Herausforderung für die Entwicklung und Validierung automatisierter Fahrfunktionen dar. Dadurch dass der Fahrer (zumindest zeitweise) die Verantwortung an die Automation übergibt, ergeben sich ganz neue Fragestellungen bezüglich der Absicherung, die bisher nicht beantwortet wurden und idealerweise einheitlich, durch einen gemeinsamen Kraftakt der Automobilindustrie (OEMs und Zulieferer) wissenschaftlich abgesichert, bearbeitet werden müssen. Besonders die von Prof. Winner (TU Darmstadt) genannte „Freigabefalle“[1] ist eine dieser Herausforderungen und erfordert, dass innerhalb der Automobilindustrie ein Umdenken stattfindet und neue Entwicklungs- und Absicherungsmethoden erforscht und angewendet werden – mit dem Ziel automatisierte Fahrfunktion wirtschaftlich zur Marktreife zu führen. 17 Partner aus Wirtschaft und Wissenschaft definieren hierzu in dem BMWi-geförderten Verbundprojekt PEGASUS neue Kriterien und Maßgaben zur Freigabe hochautomatisierter Fahrfunktionen. Zielfragestellungen des PEGASUS Projektes sind:

- **Was muss ein automatisiertes Fahrzeug leisten?**
- **Wie weisen wir nach, dass es dies auch zuverlässig leistet?**

Der nachfolgende Beitrag wird das von Continental erarbeitete Absicherungskonzept für automatisierte Fahrfunktionen darstellen und zusätzlich das geplante vorgehen innerhalb des Projektes PEGASUS genauer erläutern. Abschließend werden die daraus möglichen entstehenden Konsequenzen für die Entwicklung und Absicherung der hochautomatisierten Fahrfunktionen aufgezeigt, aus Sicht eines Zulieferers.

[1] Absicherung automatischen Fahrens | Prof. Dr. rer. nat. H. Winner | 6. FAS-Tagung München | 29. November 2013

Inhalt

1 Herausforderungen des (hoch)automatisierten Fahrens 3
2 Absicherungskonzept Continental 4
2.1 Referenz 4
2.2 Konsequenz für die Systemvalidierung 5
2.3 Simulation und Feldtests 6
3 PEGASUS 7
3.1 TP 1 Szenarienanalyse und Qualitätsmaße 7
3.2 TP 2 Umsetzungsprozesse 8
3.3 TP 3 Testen 8
3.4 TP 4 Ergebnisreflektion und Einbettung 9
4 Zusammenfassung 9

Abbildungsverzeichnis

Abbildung 1 „Schweizer Käse“ Modell 4
Abbildung 2 Objekterkennungswahrscheinlichkeit vs. Objektentfernung 5
Abbildung 3 Sensorperformance in Abhängigkeit von Umfeldparametern 6
Abbildung 4 Prinzipbild AD Architektur und Wirkkette 6
Abbildung 5 PEGASUS Projektstruktur 7
Abbildung 6 Automatisierungsrisiken 8
Abbildung 7 Eine exemplarische Darstellung des V Modells 8
Abbildung 8 Toolkette zur Absicherung von (hoch)automatisierten Fahrfunktionen 9

1 Herausforderungen des (hoch)automatisierten Fahrens

Die ansteigende Komplexität von Fahrerassistenzsystemen bis hin zu Automatisiertem Fahren ist eine enorme Herausforderung für zukünftige Verifikations- und Validierungskonzepte.

Bei heutigen Fahrerassistenzsystemen (SAE Level 2) ist der Fahrer dazu verpflichtet die Funktion dauerhaft zu überwachen (z.B. Adaptive Cruise Control (ACC)) oder die Assistenten sind für spezielle, sehr seltene Situationen i.d.R. Pre Crash Situationen entwickelt, in denen der Fahrer nicht angemessen reagiert und die Assistenten eingreifen, um einen Unfall zu verhindern oder die Auswirkungen zu mildern (z.B. Emergency Brake Assist (EBA)). Die Frage: „Wer ist besser, der Assistent oder der Mensch/Fahrer?“ stellt sich in diesen Fällen nicht.

Das hat wiederum zur Folge, dass es eine klare Trennung zwischen nominaler Funktion und Funktionaler Sicherheit gibt.

- Die ISO 26262 schließt die Leistungsfähigkeit der Funktionalität explizit aus
- Rückfallebene = Fahrer
- Probabilistische Anforderungen beschränken sich derzeit auf Hardwarefehler

Bei höheren Automatisierungsgraden (SAE Level 3 und höher) ergeben sich ganz neue Herausforderungen und Fragestellungen, da der Fahrer zumindest temporär die Fahraufgabe an das System abgibt und das System dadurch die Verantwortung für die longitudinale sowie laterale Fahraufgabe **sowie zusätzlich** die Umfeldüberwachung übernimmt. Dadurch steht der Fahrer bspw. beim hochautomatisierten als Rückfallebene nur mit ausreichendem zeitlichen Vorlauf zur Verfügung und das hochautomatisierte System muss dazu in der Lage sein alle auftretenden Situation zu erkennen und zu beherrschen.
Für eine automatisierte Fahrfunktion gilt dementsprechend:

- Die Basisfunktion (sicheres Fahren gemäß der STVO innerhalb der Funktionsgrenzen) ist sicherheitsrelevant
- Kein sofortiges Eingreifen des Fahrers, kein sofortiges Erreichen des sicheren Zustandes
- „Fail-operational“ im Gegensatz zu „fail-safe“ Systemen
- Die Integrität der Funktionalität ist sicherheitsrelevant

Allein die Vielfältigkeit der Umwelteinflüsse wie etwa Sichtverhältnisse, andere Verkehrsteilnehmer, Straßenzustände, etc. und stark nichtlineare Zusammenhänge (kleine Änderungen bei den Eingangsgrößen können massive Auswirkungen auf das Systemverhalten haben) sorgen dafür, dass die Systemreaktion als probabilistische Größe betrachtet werden muss.
Daher ergeben sich aus Verifikations- und Absicherungsperspektive hauptsächlich die folgenden Fragestellung, die auf dem Weg zur Marktreife für hochautomatisierte Systeme (SAE Level 3) zwingend beantwortet werden müssen:

- Wie gut ist gut genug? Was ist die Referenz für automatisiertes Fahren? Was ist ein akzeptables Restrisiko?
- Wie weise ich das nach? Was ist der Testumfang? Wann bin ich fertig mit Testen?

Für Fahrerassistenzsysteme (SAE Level 2) sind diese Fragen bereits beantwortet z.B. gibt es für den EBA eine automobilindustrieweite Anforderung, dass 1 False Positive Event alle 200.000 km erlaubt ist, bzw. 1 False Positive Event während eines Fahrzeuglebens. Diese eindeutige Anforderung wird normalerweise mit Field Operational Tests bei einer Fahrstrecke von ca. 1 Mio. km überprüft. Auf dieser Strecke kommt es zu 3-5 Eingriffen der Funktion, diese werden gelabelt und analysiert, ob der Eingriff gerechtfertigt war oder nicht. Jedoch werden die übrigen Kilometer der insgesamt 1Mio. km nicht auf False Negative Events untersucht, da es bisher dafür auch gar keine Notwendigkeit gab, da der Fahrer als Verantwortlicher schlussendlich bremsen muss.

Unter der Annahme, dass ein automatisiert fahrendes Systems mindestens doppelt so gut sein muss, wie der menschliche Fahrer ergibt sich laut Prof. Winner der TU Darmstadt ein Aufwand von 240 Mio. Testkilometern[2], die natürlich nicht wirtschaftlich realisiert werden können.
Aktuelle Testverfahren wie sie heute bei Fahrerassistenzsystemen zum Einsatz kommen, können entsprechend nicht ohne weiteres übernommen werden, denn für hochautomatisierte Fahrfunktionen wären sie zu zeit- und kostenintensiv und vor allem herstellerspezifisch. Mit dem Forschungsprojekt PEGASUS sollen die Resultate verschiedener Forschungs- und Entwicklungsprojekte sowie bereits existierende Fahrzeugprototypen zukünftig effizient und schnell in marktfähige Produkte überführt werden können.

2 Absicherungskonzept Continental

Das von Continental entwickelte Absicherungskonzept für automatisierte Fahrfunktionen adressiert die oben genannten Fragestellungen und zeigt mögliche Antworten auf. Ausgehend von den Herausforderungen des (hoch-)automatisierten Fahrens, z.B. die Übergabe der Fahraufgabe vom Menschen zum System, über eine Referenzdiskussion, hin zu den daraus resultierenden Konsequenzen für die Systemauslegung, Systementwicklung und schlussendlich die Systemvalidierung.

2.1 Referenz

Wie bei allen technischen Systemen, wird auch beim automatisierten Fahren eine 100%ige Lösung und damit auch eine 100%ige Sicherheit nicht möglich sein. Dies hat zur Konsequenz, dass dringend ein Konsens über die gesellschaftliche Akzeptanz über mögliche Restrisiken herbeigeführt werden muss und das Restrisiko quantifiziert wird. Continental hat sich ausführlich mit der Fragestellung der gesellschaftlichen Akzeptanz auseinandergesetzt und den Menschen als Referenzgröße definiert. Vor Allem sind dabei die Fahrsituationen für die Referenzbetrachtung interessant, bei denen menschliche Fahrer versagt haben und es zu Unfallereignissen gekommen ist. Dazu wurden ausführlich Unfalltypen, Unfallarten und die jeweiligen Auftretenswahrscheinlichkeiten analysiert sowie die Verkettung von Ereignissen untersucht, die in einem Unfall enden können. Das sogenannte Schweizer Käse Modell[3] beschreibt die Entstehung von Unfällen sehr anschaulich und verdeutlicht, dass Unfälle i.d.R. eine Verkettung von unglücklichen Umständen sind. Abbildung 1 verdeutlicht das Prinzip des Schweizer Käse Modells.

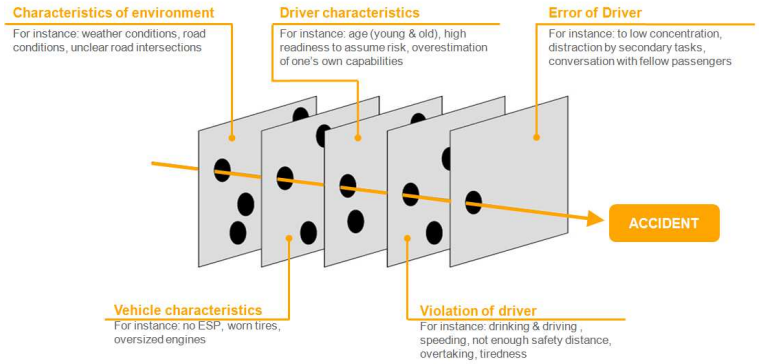

Abbildung 1 „Schweizer Käse" Modell

Continental stellt zur Diskussion, dass eine mögliche Referenzwahrscheinlichkeit für ein automatisiertes System (= gesellschaftlich akzeptables Restrisiko) mit der Wahrscheinlichkeit eines Unfallereignisse, versursacht durch PKW mit mindestens einem Getötetem auf der Autobahn gleichzusetzen ist. Zumindest für den naheliegenden Anwendungsfall des automatisierten Fahrens auf

[2] Handbuch Fahrerassistenzsysteme | Winner, Hermann, Hakuli, Stephan, Wolf, Gabriele (Hrsg.) | Springer Vieweg Verlag ISBN 978-3-8348-9977-4

Autobahnen. Die Größenordnung für solch ein Ereignis ist bei 10^{-8}/h. Absolut gibt es ~170 solcher Unfälle pro Jahr auf deutschen Autobahnen mit ~200 Getöteten.
Das gerade beschriebene Vorgehen wird nur dazu verwendet, um festzulegen wie gut das System sein muss und beantwortet zumindest teilweise die erste Frage: „Was muss ein automatisiertes System leisten?“. Ein weiterer wichtiger Bestandteil der Antwort auf diese Frage ist, dass für ein automatisiertes System Szenarien und Situationen schwierig beherrschbar sein können, die bisher nicht in der Unfallstatistik enthalten sind, da die Beherrschung dieser Szenarien keinerlei Schwierigkeiten für den Menschen darstellen. Um dieses Automatisierungsrisiko zu quantifizieren muss eine Methodik erarbeitet werden, mit der die für die Automatisierung schwierigen und kritischen Szenarien identifiziert und beschrieben werden. Continental erarbeitet aktuell eine Methodik, um das Automatisierungsrisiko zu quantifizieren (wie andere Zulieferer und OEMs auch) und die Szenarien zu beschreiben. Idealerweise sollte diese Methodik und folglich auch die Beschreibung dieser Szenarien gemeinschaftlich erarbeitet werden, was aktuell Bestandteil des PEGASUS Projektes ist. Mehr zum Projekt PEGASUS in Kapitel 3.

2.2 Konsequenz für die Systemvalidierung

Aus Absicherungsperspektive sind zwei Aspekte von entscheidender Bedeutung:

1. **Loss of function**
2. **Loss of integrity**

Der Verlust der Funktion kann z.B. durch den Ausfall eines Steuergerätes verursacht werden, was z.B. das Lenkungssteuergerät sein könnte. Da dem Fahrer wie oben beschrieben eine gewisse Zeit zur Übernahme gegeben werden muss, muss das System fallbackfähig sein und zumindest in den entscheidenden Bereichen redundant ausgelegt werden. Dieser Bereich ist über die ISO 26262 abgedeckt.
Der zweite Punkt „Loss of integrity“ ist bei dem Thema Absicherung für das automatisierte Fahren entscheidend. So kann z.B. ein Objekterkennungsalgorithmus ein Objekt nicht identifizieren, was unterschiedlichste Ursachen haben kann, obwohl kein Fehler innerhalb des Systems vorliegt.
Die in Kapitel 2 geführte Referenzdiskussion findet für diese Fälle Anwendung. Dabei wird das System so ausgelegt, dass ein Verlust der Integrität maximal mit einer Wahrscheinlichkeit, die der Referenzwahrscheinlichkeit entspricht, auftreten darf. Mit Hilfe der Fehlerbaummethodik lassen sich diese Wahrscheinlichkeiten auf Teilsysteme und Algorithmen verteilen und so Anforderungen für einen Objekterkennungsalgorithmus herleiten. Eine mögliche Anforderung könnte dann lauten: „Der Radar muss Objekte mit einer Wahrscheinlichkeit von 99,99% in Entfernung X erkennen“. Abbildung 5 verdeutlicht die Wahrscheinlichkeit der Objekterkennung in Abhängigkeit zur Objektentfernung.

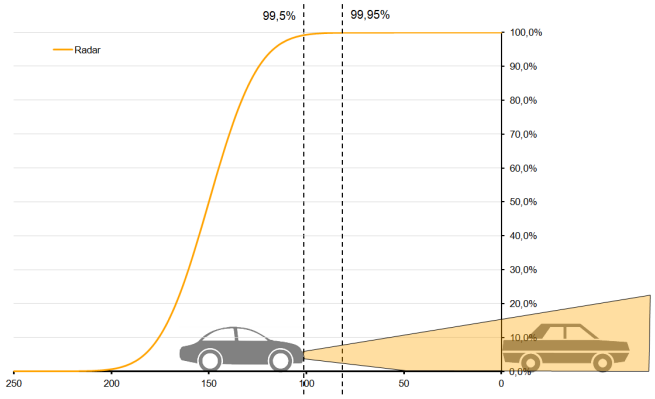

Abbildung 2 Objekterkennungswahrscheinlichkeit vs. Objektentfernung

Dabei muss zwingend sichergestellt werden, dass unter allen relevanten Umweltbedingungen diese Objekterkennungswahrscheinlichkeit eingehalten wird. Falls die Objekterkennung dabei einen

kritischen Wert erreicht (mögliche Systemgrenze), muss das System dieses erkennen und die Fahrerübernahme rechtzeitig initiieren. Abbildung 3 verdeutlicht dieses.

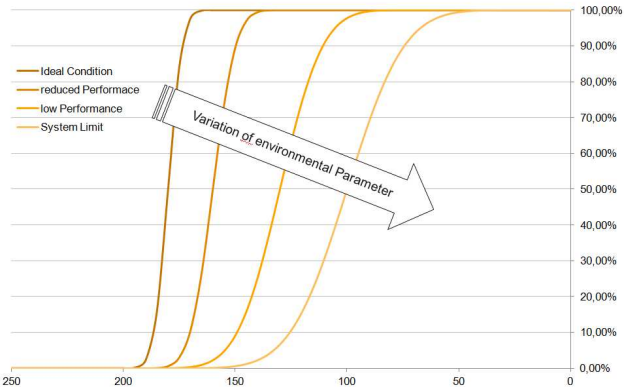

Abbildung 3 Sensorperformance in Abhängigkeit von Umfeldparametern

Weiterhin muss sichergestellt werden, dass das gesamte Sensorsetup diversitär redundant ausgelegt wird. Das bedeutet (vereinfacht dargestellt), dass unterschiedliche Sensortechnologien (z.B. Radar, Lidar, Kamera, usw.) für das Sensorsetup verwendet werden und sichergestellt wird, dass diese Technologien nicht dieselben Einschränkungen haben bei der Objekterkennung.

2.3 Simulation und Feldtests

Durch das Anwenden dieser Methodik wird sichergestellt, dass die Inputgrößen für das gesamte System valide sind. Dies erlaubt, dass die weitere Wirkkette nach der Objekterkennung z.B. bestehend aus Objektfusion, Fahrstrategie, Trajektorienplaner und der Aktuatorik in der Simulation überprüft und getestet werden können, was einen erheblichen Beitrag zur Reduzierung der notwendigen Absicherungskilometer zur Folge hat. Abbildung 4 verdeutlicht das Prinzip.

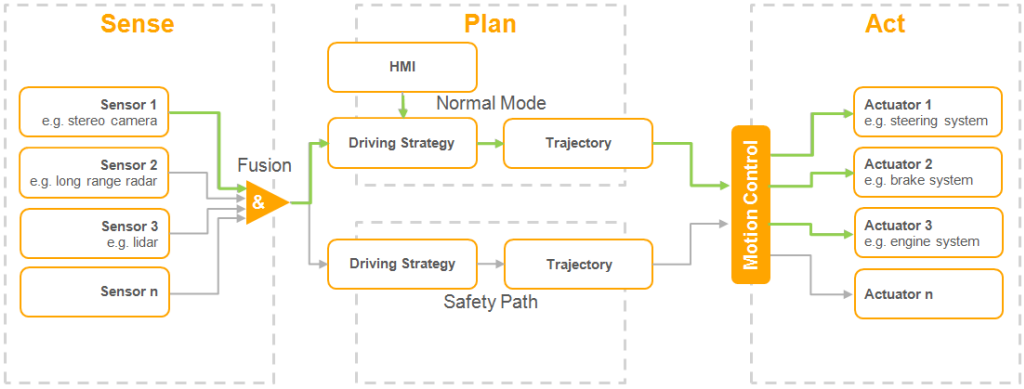

Abbildung 4 Prinzipbild AD Architektur und Wirkkette

Das konsequente Anwenden der Methodik und die intelligente Verteilung der Tests auf Simulation und natürlich auch Field Operational Tests wird entscheidend sein, die Absicherungsaufwende deutlich zu reduzieren und (hoch)automatisierte Fahrfunktionen zur Marktreife zu führen.

3 PEGASUS

In PEGASUS (Projekt zur Etablierung von generell akzeptierten Gütekriterien, Werkzeugen und Methoden sowie Szenarien und Situationen zur Freigabe hochautomatisierter Fahrfunktionen) werden im Zeitraum seit Januar 2016 bis Juni 2019 allgemein akzeptierte Methoden und Werkzeuge für die Absicherung hochautomatisierter Fahrzeugfunktionen entwickelt und am Beispielsystem Autobahn-Chauffeur demonstriert. Zu den 17 Partnern gehören innovative KMUs, OEMs und Zulieferer sowie Forschungseinrichtungen.
PEGASUS hat sich zum Ziel gesetzt zwei entscheidende Fragen aus Sicht des automatisierten Fahrens zu beantworten:

- **Was muss ein automatisiertes Fahrzeug leisten?**
- **Wie weisen wir nach, dass es dies auch zuverlässig leistet?**

Um diese Fragen beantworten zu können, ist folgende Projektstruktur mit vier Teilprojekten (TP) entstanden:

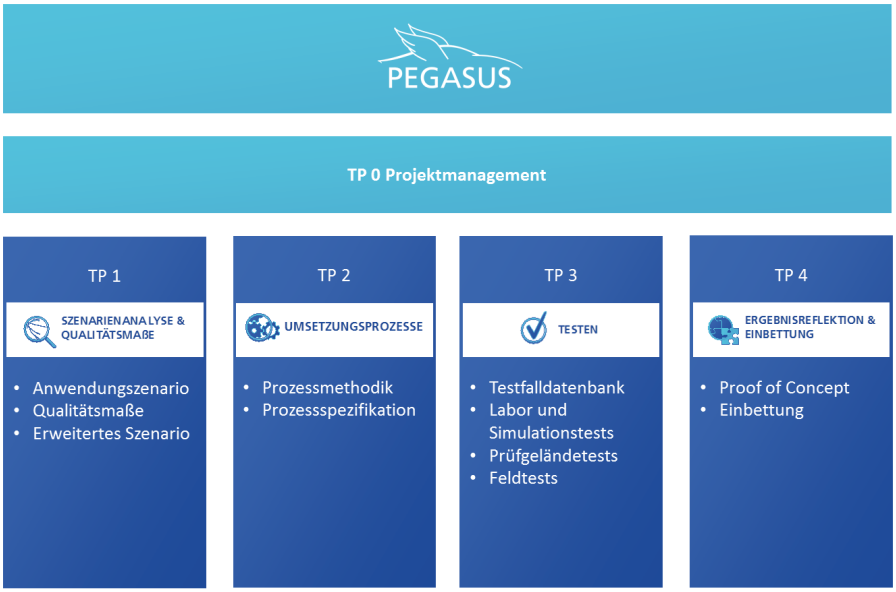

Abbildung 5 PEGASUS Projektstruktur

3.1 TP 1 Szenarienanalyse und Qualitätsmaße

Die Entwicklung eines erfolgreichen Vorgehens zum Testen von hochautomatisierten Fahrfunktionen (HAF) beruht auf der Analyse der zu testenden Szenarien sowie der Definition geeigneter Kriterien und Maße zur Beurteilung der Qualität. Sollen Prozesse, Methoden und Werkzeuge anhand von Anwendungsfällen erprobt und evaluiert werden, die selbst aber noch Gegenstand der Forschung und Entwicklung sind, so können im Allgemeinen schwer Qualitätsmaßstäbe hierfür definiert werden. Deshalb baut PEGASUS auf dem zukunftsnahen Beispielsystem Autobahn-Chauffeur auf. Diese Funktion wird in TP 1 aufgegriffen, gezielt erweitert und konkretisiert. Das Ergebnis ist ein umfassendes Szenario für ein hochautomatisiertes Fahrzeug auf der Autobahn. Die Arbeitsergebnisse stützen sich dabei nicht nur auf technische Analysen, sondern beruhen auch auf Erkenntnissen aus menschzentrierten Untersuchungen. Mit einer zu entwickelnden Methodik zur Ermittlung der maschinellen sowie menschlichen Leistungsfähigkeit wird es möglich, das notwendige Sicherheitsniveau zu ermitteln. Die dabei definierten Kriterien, Qualitäts- und Gütemaße bilden die Basis für das weitere Testen.

Eine der Herausforderungen beim Automatisierten Fahren sind die Risiken, die durch die Automatisierung entstehen und nur schwer quantifizierbar sind. Innerhalb von PEGASUS wird eine Methodik entwickelt diese Risiken zu identifizieren und zu beurteilen. Abbildung 6 verdeutlicht das Automatisierungsrisiko.

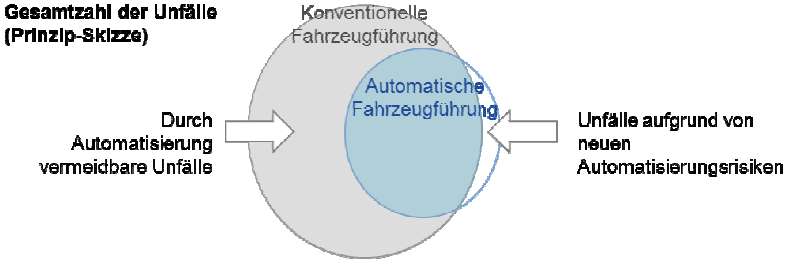

Abbildung 6 Automatisierungsrisiken

Mit der Betrachtung weiterer Systeme wird die Übertragbarkeit des Vorgehens auf weitere Anwendungssituationen und Fahrzeugfunktionen sichergestellt und ein skalierbarer Ansatz kann vorgeschlagen werden.

3.2 TP 2 Umsetzungsprozesse

Die Identifikation und Erstellung möglichst allgemeingültiger Entwicklungs- sowie Testprozesse liegt als Querschnittsthema im Fokus des TP 2. Ausgehend von den Kriterien und Maßen aus TP 1 erfolgt die Analyse des Modifikationsbedarfes existierender Kriterien, Metriken und Prozesse (u.a. beim Nachweis der funktionalen Sicherheit) wie sie bereits in der Automobilindustrie etabliert sind. Ergänzend erfolgt im Zusammenwirken mit TP 1 eine Betrachtung innovativer Ansätze und Konzepte zur Analyse neuartiger Automatisierungssysteme. Die Umsetzungsprozesse werden dem schrittweisen Vorgehen des automobilen Entwicklungsprozesses im Rahmen des V-Modells Rechnung tragen und für industrielle Prozesse ausreichend flexibel sein. Zudem müssen sie auch ausreichend robust für den Einsatz im Rahmen der Serienentwicklung sein. Eine diesbezügliche Schärfung der Ansätze erfolgt u.a. durch das Einbeziehen von Rückkopplungsschleifen bzw. -ebenen im V-Modell (vgl. bsph. Abbildung 7).

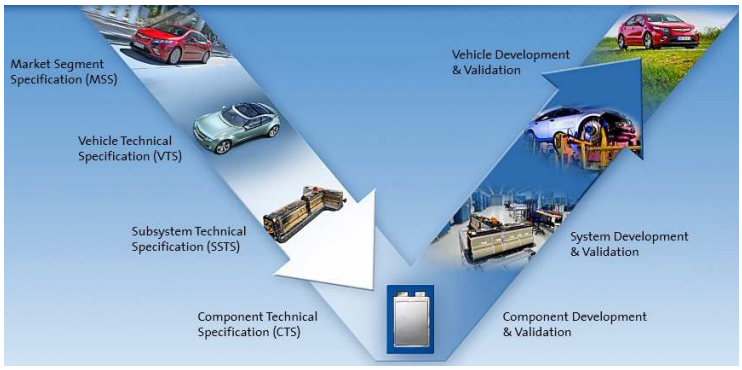

Abbildung 7 Eine exemplarische Darstellung des V Modells

3.3 TP 3 Testen

Im TP 3 liegt der Fokus auf der Umsetzung der Testaufgaben mit Hilfe von konkreten Testmethoden und Testverfahren für die Bereiche Simulation/Labore/Prüfstände, Prüfgelände und Feldtests. Es wird dabei auf den nach Auftretenswahrscheinlichkeit und Gefahrenpotential bewerteten Szenarien-Klassen des Verkehrsumfeldes aufgesetzt, in dem sich ein hochautomatisiert fahrendes Fahrzeug bewegt. Der Nachweis, dass diese Situationen hinreichend sicher beherrscht werden, soll mit den hier

erarbeiteten Testmethoden, -verfahren und realen Erprobungen geführt werden können. Für die Bewertung, ob die Beherrschung „hinreichend sicher“ ist, wird auf Kriterien und Maße zurückgegriffen, die in TP 1 unter Bezugnahme auf die menschlichen Fähigkeiten ermittelt und festgelegt werden. Weiterhin fließen Erkenntnisse aus TP 2 ein, welche insbesondere die zusätzlichen, aus der Automatisierung entstehenden besonderen Prüfaufgaben definieren. Bei der Festlegung der Prüfumfänge muss weiterhin unterschieden werden, welche Tests im Labor durch Simulation (Hardware In the Loop (HIL), Software In the Loop (SIL), …) durchgeführt werden können, welche auf dem Prüfgelände durchgeführt werden und welche durch Absicherung im Feld umgesetzt werden müssen. Erkenntnisse aus der Durchführung der Tests fließen während der Projektlaufzeit von PEGASUS direkt in eine verbesserte Spezifikation der Tests ein. Dies betrifft insbesondere Grenzen der Anwendbarkeit von festgelegten Kriterien und Maßen bzw. Prüfmethoden sowie Erkenntnissen über die notwendige Prüftiefe. Abbildung 8 veranschaulicht die gerade beschriebene Toolkette.

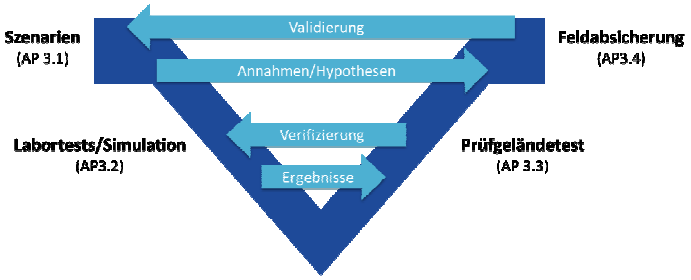

Abbildung 8 Toolkette zur Absicherung von (hoch)automatisierten Fahrfunktionen

3.4 TP 4 Ergebnisreflektion und Einbettung

Das TP 4 Ergebnisreflektion und Einbettung wird in „Proof of Concept“ sowie in „Einbettung“ aufgeteilt. Die Durchführung des Teilprojekts erfolgt parallel zu den anderen Teilprojekten und beleuchtet kritisch die Arbeitsergebnisse. Ziel ist die Gewährleistung eines Testniveaus, mit dem Produkte für den Straßenverkehr bzw. zur Nutzung durch Kunden zugelassen werden können. Eine Feedback-Schleife zur Projektlaufzeit sorgt dabei für einen systematischen Informationsrückfluss in PEGASUS hinein, sodass dieser dort entsprechend aufgegriffen und bei der Einbettung der Ergebnisse in die Partnerstrukturen berücksichtigt werden kann.

4 Zusammenfassung

Es ist der richtige (und notwendige!) Schritt, dass die deutsche Automobilindustrie im Schulterschluss mit der Wissenschaft gemeinschaftlich der Herausforderung zur Validierung automatisierter Fahrfunktionen für Markteinführung stellt und gemeinsam ein einheitliches Vorgehen und somit einen neuen state-of-the-art entwickelt. Die gemeinsame Beantwortung der zu Anfang gestellten Fragen

- **Wie gut ist gut genug?**
- **Wie muss der Nachweis geführt werden?**

reduziert insbesondere das individuelle Risiko der jeweiligen OEMs und Zulieferer und wird die Basis für die Markteinführung dieser komplexen Technologie sein.