#78 SPECTRUM

Liebe Leserinnen und Leser,

Software nimmt in der heutigen Mobilität einen wesentlichen Stellenwert ein. Zukünftig werden neben nachhaltigen Antriebstechnologien vor allen Dingen softwarebasierte Innovationen über den Erfolg neuer Mobilitätslösungen entscheiden. Mit der Marke FEV.io haben wir diesem technologischen Trend Rechnung getragen und unsere Softwarekompetenzen gebündelt. Ein Eindruck dieser Kompetenz, die wir global etabliert haben, erwartet Sie auf den folgenden Seiten.

Bei der automobilen Cybersecurity bieten wir beispielsweise unseren Kunden einen ganzheitlichen Ansatz an. Wir präsentieren Ihnen in diesem SPECTRUM, wie wir sicherstellen, dass zukünftige Fahrzeuge den Vorschriften hinsichtlich der Cybersecurity entsprechen und optimal gegen entsprechende Bedrohungen gerüstet sind.

Auch der Bedarf an Aktualisierungen und Erweiterungen von softwaredefinierten Funktionen wächst, etwa beim Typgenehmigungsverfahren von Fahrzeugen. Wir präsentieren Ihnen einen virtuell durchgeführten Entwicklungs- und Validierungsansatz, der konkret homologationsrelevante Softwareaktualisierungen ermöglicht und erheblichen Zeit- und Kostenaufwand einspart.

Außerdem geben wir Ihnen einen Überblick zu den Leistungen im Bereich ADAS/AD, die wir ganzjährig in unserem Testzentrum in Marokko anbieten. In einem weiteren Artikel gehen wir am Beispiel von FEV.io in Indien auf den Ausbau globaler Softwarekompetenzen ein, um die Beschleunigung von Innovationen im Bereich der intelligenten Mobilität sicherzustellen.

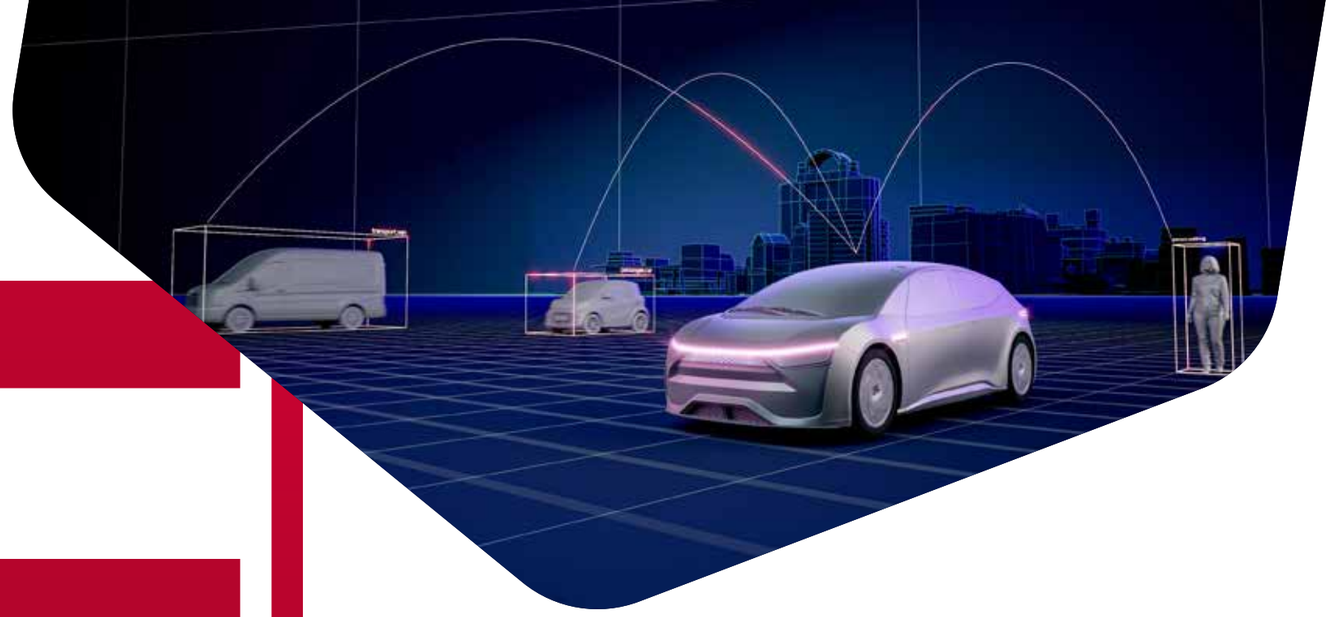
Neben Softwarelösungen steht FEV unverändert für innovative Lösungen bei der Gesamtfahrzeugentwicklung. Mit FEVs „PD-HVX" stellen wir in dieser Ausgabe eine Lösung zum Aufspüren von elektrischer Teilentladung in Hochvolt-Fahrzeugantrieben vor, die zeit- und kostenintensive Fahrzeugausfälle bereits während des Entwicklungsprozesses vermeiden kann. Außerdem geben wir Einblicke in eine Kooperation mit Iveco, deren Ziel die Entwicklung einer vollständig flexiblen und modularen batterieelektrischen Plattform für leichte Nutzfahrzeuge war.

Mit der neuen Serie „Proprietäre Lösungen" unterstreichen wir unsere Philosophie „Feel EVolution" und präsentieren Ihnen einzigartige Innovationen, die unsere Experten für spezifische aktuelle Herausforderungen entwickelt haben.

Ich wünsche Ihnen eine spannende Lektüre,
die Sie inspiriert.

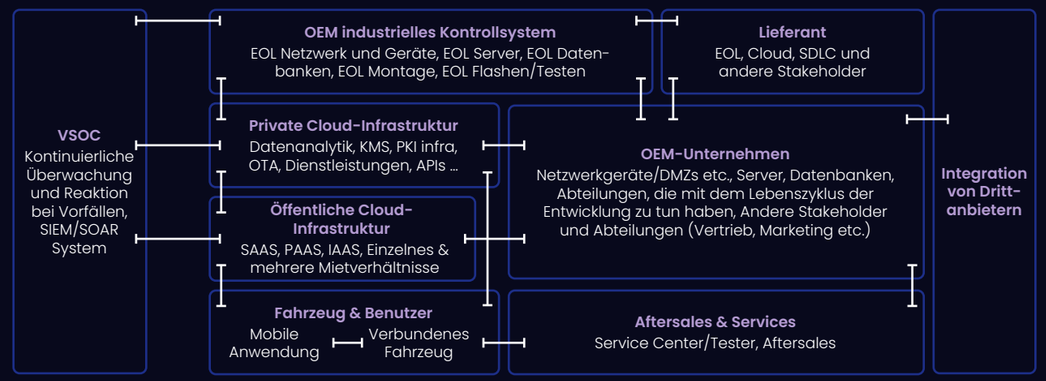
Dr. Norbert W. Alt
Chief Operating Officer (COO) und
Geschäftsführer der FEV Group

CONTENT



#1 *FEV.io* – Ein verlässlicher Partner für *Cybersecurity in der Automobil-industrie*

Die Automobilindustrie befindet sich aufgrund der rasanten Entwicklung hochmoderner Technologien und komplexer Softwarelösungen im Wandel. Besonders deutlich wird dies bei der Entwicklung von vernetzten Fahrzeugen. Abbildung 1 veranschaulicht das Ökosystem eines vernetzten Fahrzeugs und zeigt den Weg vom Originalhersteller (Original Equipment Manufacturer, OEM) zum Nutzer. Dieses Ökosystem verdeutlicht die Bedeutung der Cloud-Infrastruktur bei der Verwaltung von Fahrzeugdaten, der Möglichkeit von Over-the-Air-Updates und der Bereitstellung von After-Sales-Services. Integrationen von Drittanbietern erweitern die Möglichkeiten des Ökosystems und gewährleisten ein nahtloses Nutzererlebnis und kontinuierlichen Fahrzeugsupport.



1.
Automotive Cybersecurity Ökosystem.

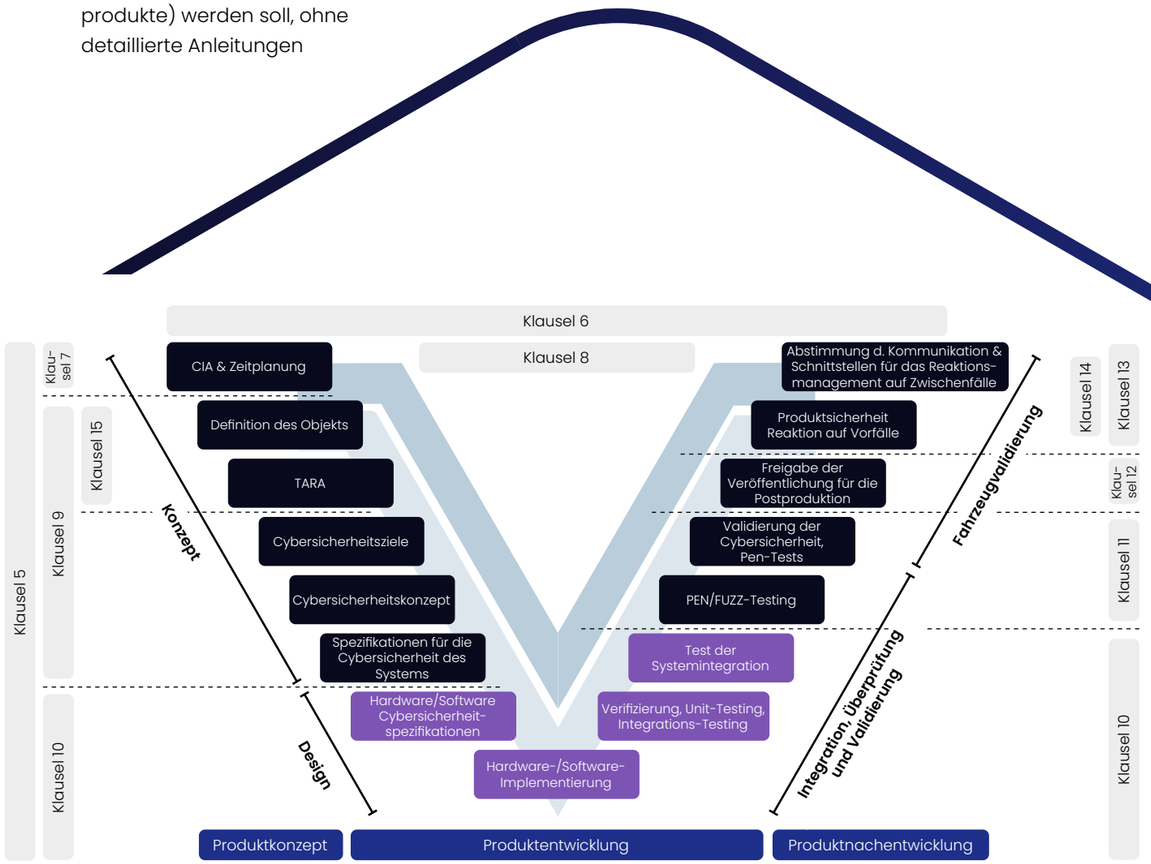
Durch die Einführung fortschrittlicher Technologien und Softwarelösungen sind moderne Fahrzeuge jedoch anfällig für Bedrohungen geworden, die z. B. die Fahrzeugsicherheit, den Datenschutz oder die Gesamtfunktionalität des Fahrzeugs beeinträchtigen können.

Der Schutz moderner Fahrzeuge vor potenziellen Bedrohungen fällt unter die Disziplin der Cybersecurity (Cybersicherheit). Die International Organization for Standardization, ISO hat den Bedarf an standardisierten Cybersicherheitspraktiken für den Automobilbereich erkannt und in Zusammenarbeit mit SAE International im Jahr 2021 die ISO/SAE 21434 eingeführt. Sie dient als eine der wichtigsten Referenzen für OEMs und Zulieferer zur Einhaltung von Cybersicherheitsvorschriften wie UNECE R155.

Die Umsetzung der in ISO/SAE 21434 beschriebenen Anforderungen kann eine große Herausforderung sein, insbesondere weil die Norm oft vorgibt, was erreicht (Anforderungen) und geliefert (Arbeitsprodukte) werden soll, ohne detaillierte Anleitungen zu geben, wie dies zu tun ist. An dieser Stelle wird FEV.io zu einem wichtigen Partner. Mit einem Team von Experten können Kunden durch den gesamten Lebenszyklus geführt werden, einschließlich der Durchführung von Sicherheitsrisikoanalysen, der Implementierung von Cybersicherheitskontrollen und -anforderungen sowie der Durchführung von Verifizierungs- und Validierungsaktivitäten.

ISO/SAE 21434 Klauseln und Aktivitäten innerhalb des V-Modells

Die Norm ISO/SAE 21434 besteht aus 15 Klauseln, in denen Cybersicherheitsaktivitäten in Form von Anforderungen und Arbeitsprodukten von der Konzeptphase bis zur Stilllegung beschrieben werden. Darüber hinaus besteht ISO/SAE 21434 aus Aktivitäten des Cybersicherheitsmanagements. Abbildung 2 veranschaulicht, wie spezifische Klauseln und ihre entsprechenden Aktivitäten aus ISO/SAE 21434 in das V-Modell integriert werden. Diese Abbildung bietet einen guten Überblick über die Verteilung der Cybersicherheitsaktivitäten auf die verschiedenen Phasen und benennt die für diese Aktivitäten verantwortlichen Akteure auf Hersteller- sowie auf Zuliefererseite.



2
ISO/SAE 21434-Klauseln und Aktivitäten innerhalb des V-Modells.

»FEV.io verfügt über eine systematische Methodik, die eine genaue Identifizierung von Assets, Bedrohungsszenarien und Angriffswegen beinhaltet und potenzielle Risiken bewertet.«

Eine systematische Methodik für die Analyse von Sicherheitsrisiken

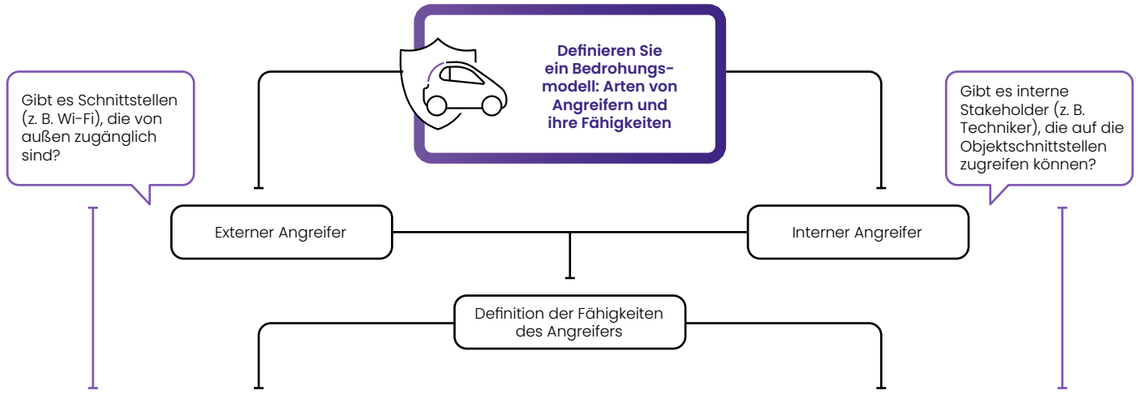
Die Konzeptphase ist eng mit dem Grundsatz „Security-by-design" verknüpft. Bei diesem Prinzip geht es darum, Sicherheitsüberlegungen (z. B. Anforderungen und Kontrollmechanismen) von Anfang an in das zu analysierende System (genannt „Objekt") einzubeziehen. Zu diesem Zweck besteht die Konzeptphase aus mehreren Aktivitäten, darunter die Durchführung einer Sicherheitsrisikoanalyse (Threat Analysis and Risk Assessment, TARA) des Objekts. Die TARA besteht aus sieben Aktivitäten, darunter die

a. Identifizierung des zu schützenden Objekts,

b. Ermittlung potenzieller Bedrohungen für das identifizierte Objekt (Bedrohungsszenarios) und

c. Ermittlung der von einem Angreifer durchgeführten Aktionen zur Realisierung einer Bedrohung (Angriffspfadanalyse).

Im Folgenden wird ein Einblick in die Durchführung dieser Aktivitäten gegeben. FEV.io hat eine systematische Methodik für die Durchführung der TARA. Die Methodik zielt darauf ab, einen umfassenden Satz von Assets zu haben. Dieser Satz besteht aus generischen Assets und spezifischen Assets. Erstere bezeichnen Assets, die auf jedes elektronische Steuergerät (ECU) anwendbar sind, wie z. B. Software-Updates und Diagnose-Routing. Letztere bezeichnen Assets, die spezifisch für das zu analysierende Element sind, wie z. B. Nachrichten, die von den für das Objekt relevanten Kommunikationskanälen übertragen werden. Dieser Prozess der Identifizierung spezifischer Assets verläuft von einer grobkörnigen Analyse, bei der nur ein generischer Kommunikationskanal als Asset identifiziert wird, zu einer detaillierteren, feinkörnigen Analyse. Bei letztgenannter Analyse werden spezifische Nachrichten identifiziert. Sie führt zu praktikableren Lösungen, die sich auf den Schutz nur einer Teilmenge der über einen Kommunikationskanal übertragenen Nachrichten konzentrieren und nicht auf die gesamte Menge, was aus Effizienzgründen unpraktisch sein könnte.



3
Bedrohungsmodellbasierter Ansatz.

Für die Identifizierung von Bedrohungsszenarien verwendet die Methodik von FEV.io einen auf einem Bedrohungsmodell basierenden Ansatz, der in Abbildung 3 dargestellt ist. Ein Bedrohungsmodell besteht aus Annahmen darüber, welche Angreifer in Betracht gezogen werden und welche Fähigkeiten sie haben, um das Objekt zu kompromittieren. Nach der Fertigstellung des Bedrohungsmodells und der Genehmigung durch den Kunden identifiziert ein Expertenteam anhand des Modells nahtlos Bedrohungen und die entsprechenden Angriffsflächen.

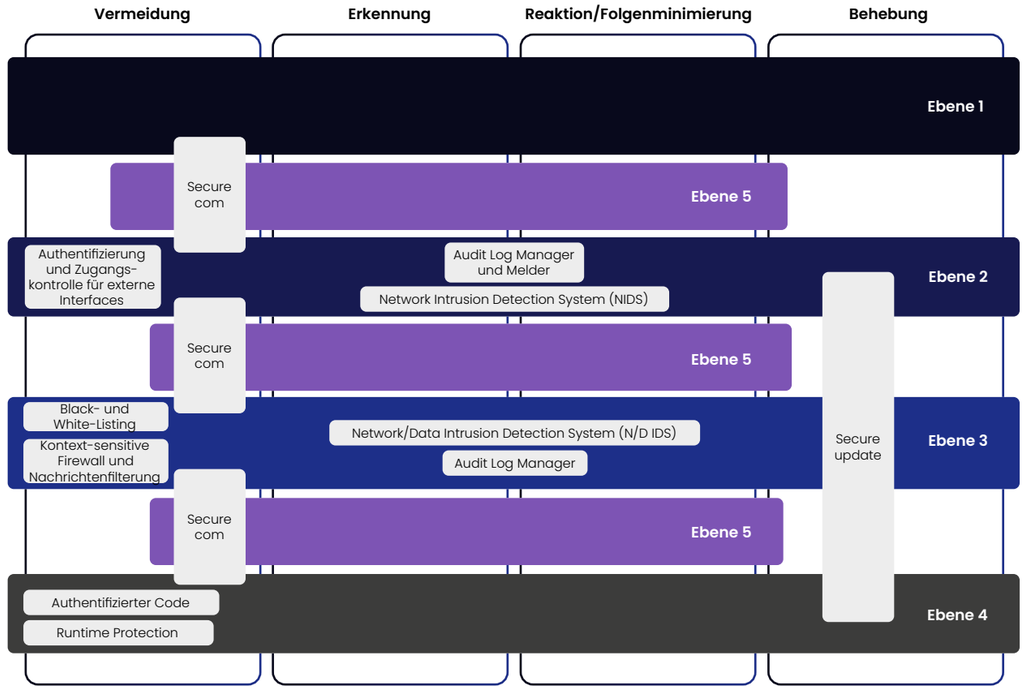
FEV.io nutzt diesen Ansatz, um die Aufzählung der Angriffspfade für die identifizierten Bedrohungsszenarien zu erleichtern. Basierend auf dem Typ des Angreifers und seinen entsprechenden Fähigkeiten werden die folgenden Fragen analysiert, wobei die Systemarchitektur als Eingangsinformation dient. Antworten auf diese Fragen dienen als Grundlage für die Beschreibung der möglichen Vorgehensweisen eines Angreifers.

- **Wie erreicht der Angreifer die Angriffsfläche?**
- **Wie geht der Angreifer vor, um von der Angriffsfläche aus zu dem Asset zu gelangen?**
- **Wie geht der Angreifer vor, um die Cybersicherheits-eigenschaft des Assets zu verletzen?**

Ein wesentlicher Vorteil der Beschreibung von Angriffspfaden auf der Grundlage solcher Fragen ist die Möglichkeit, Empfehlungen für Sicherheitsmaßnahmen zu erstellen. Diese Empfehlungen können sorgfältig an einem oder mehreren Orten innerhalb der Systemarchitektur eingesetzt werden, z. B. an der Angriffsfläche oder an jedem anderen geeigneten Ort, den der Angreifer nutzt, um das Objekt zu erreichen.

Zusätzlich hat FEV.io eine Defense-in-Depth-Strategie entwickelt (Abb. 4). Diese Strategie nutzt eine Cybersicherheitsarchitektur mit mehrschichtigen Verteidigungsmaßnahmen zum Schutz von Informationssystemen. Sie wurde von Experten entwickelt und umfasst sichere Kommunikation, authentifizierten Zugriff und Angriffserkennung, um Bedrohungen zu adressieren. Kontextabhängige Firewalls und authentifizierte Codeausführung erhöhen die Widerstandsfähigkeit und unterstreichen die entscheidende Rolle der Architektur beim Schutz vor ausgeklügelten Cyberangriffen.

Zusammengefasst verfügt FEV.io über eine systematische Methodik für die Konzeptphase, die eine genaue Identifizierung von Assets, Bedrohungsszenarien und Angriffswegen beinhaltet. Durch die Anwendung dieser Methodik wird eine gründliche Analyse gewährleistet, die zur Bewertung potenzieller Risiken führt. Infolgedessen kann FEV.io fundierte Empfehlungen zu Cybersicherheitszielen, Kontrollmechanismen und Anforderungen abgeben, um die identifizierten Risiken zu verringern.



4
FEV.io Tiefenverteidigungsstrategie.

Absicherung der Produktentwicklungsphase

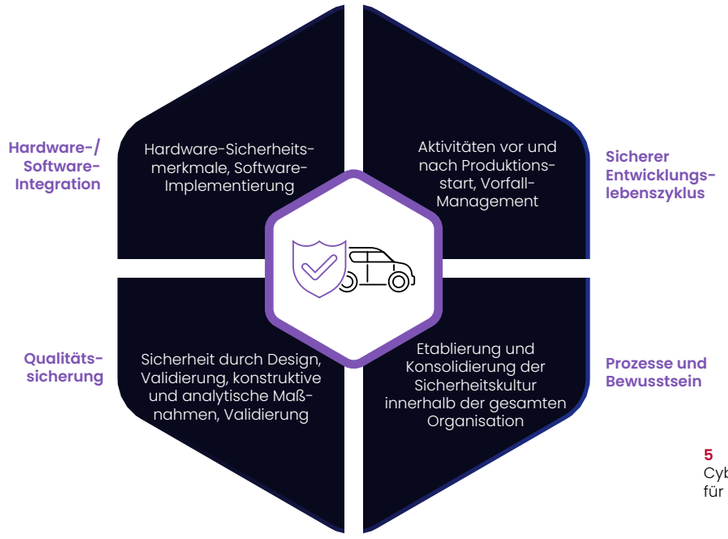
Um eine sichere Produktion zu gewährleisten, müssen robuste Kontrollmechanismen wie Secure Boot und Secure Flashing eingesetzt werden. Einerseits werden beim sicheren Booten kryptografische Verfahren eingesetzt, um die Authentizität der auf den Steuergeräten laufenden Software zu überprüfen und so die Ausführung von manipulierter Software zu verhindern. Auf der anderen Seite garantiert sicheres Flashen, dass nur legitimierte und authentifizierte Firmware-Updates angewendet werden, wodurch z. B. Spoofing-Angriffe verhindert werden, die darauf abzielen, bösartigen Code über nicht autorisierte Firmware-Updates in das Gerät zu flashen. FEV.io entwickelt derartige Kontrollmechanismen, beispielsweise einen einzigartigen sicheren Boot-Mechanismus, der asymmetrische Kryptografie verwendet und eine zusätzliche Schutzebene im Vergleich zu traditionellen Boot-Mechanismen bietet. Die von den Endbenutzern des Produkts geforderte Leistung wird dabei nicht beeinträchtigt.

Um die Sicherheit von Fahrzeugnetzwerken zu verbessern und vor potenziellen Sicherheitslücken zu schützen, widmet sich FEV.io der Entwicklung robuster Mechanismen zur effektiven Verwaltung des Zugriffs auf und der Nutzung von Ressourcen und Daten des zu entwickelnden Objekts. Diese Mechanismen werden auch als Zugriffskontroll- und Nutzungskontrollmechanismen bezeichnet.

Erstere regeln, welche Aktionen Benutzer durchführen und auf welche Ressourcen sie innerhalb des Objekts zugreifen dürfen. Letztere legen fest, wie autorisierte Benutzer mit den Ressourcen und Daten interagieren dürfen, sobald sie Zugang erhalten haben. Die Entwicklung von Zugangs- und Nutzungskontrollmechanismen ist unerlässlich, um verschiedene Angriffe zu verhindern, insbesondere Angriffe zur Erhöhung der Zugriffsrechte.

Bei der Verifizierung verfolgt FEV.io einen dualen Ansatz, um potenzielle Softwareprobleme zu identifizieren. Zunächst werden statistische Analysewerkzeuge eingesetzt, um die Codebasis zu analysieren, ohne sie auszuführen. So werden beispielsweise potenzielle Fehler oder bösartige Informationsflüsse identifiziert. Dieser Ansatz wird durch dynamische Testwerkzeuge ergänzt. Beim dynamischen Testen wird die Software in unterschiedlichen Laufzeitumgebungen ausgeführt, um potenzielle Laufzeitprobleme wie Speicherlecks oder andere Probleme zu identifizieren, die bei statischen Tests möglicherweise nicht erkannt werden.

FEV.io verfügt über eine große Erfahrung in der Durchführung von Validierungsaktivitäten wie Fuzz- und Penetrationstests, die von Kunden und Partnern geschätzt wird. In einem früheren Projekt wurde zum Beispiel bei Fuzz-Testverfahren eine potenzielle Overflow-Schwachstelle im CAN-Kommunikationsprotokoll eines Fahrzeugs entdeckt. Es wurden in Folge sofort Abhilfemaßnahmen ergriffen, die eine erhebliche Haftung und ein potenzielles Sicherheitsrisiko beseitigten, noch bevor das Fahrzeug in Produktion ging.



5
Cybersicherheitsrahmen für OEMs und Tier 1s.

Zusätzlich bietet FEV.io einen Rahmen für die Cybersicherheitsstrategie (Abb. 5). Er umfasst die Integration von Hardware- und Softwaresicherheit, Qualitätssicherung durch Design und Validierung sowie einen sicheren Entwicklungszyklus. Es ist entscheidend, Aufmerksamkeit sowohl vor als auch nach der Produktion sicherzustellen und eine Unternehmenskultur zu etablieren, die Sicherheit in den Mittelpunkt stellt.

Kontinuierliches Engagement für die Entwicklung nach der Markteinführung

Das Engagement von FEV.io für die Cybersicherheit geht weit über die Konzept- und Entwicklungsphase hinaus. In der Betriebs- und Wartungsphase sorgen Experten für den Schutz von Over-The-Air-Updates (OTA) durch Verschlüsselung und digitale Signaturen, um die Integrität und Vertraulichkeit der Software zu gewährleisten. Systeme zur Erkennung von Angriffen (Intrusion Detection) überwachen kontinuierlich die bordeigenen Netze, um potenzielle Bedrohungen schnell zu erkennen und darauf zu reagieren. Regelmäßige Sicherheitsprüfungen und Audits sorgen dafür, dass die Software auch nach der Einführung sicher bleibt.

Selbst während der Stilllegungsphase achtet FEV.io darauf, alle Daten sicher zu löschen, um jeglichen Missbrauch von verbleibenden privaten oder geschützten Informationen zu verhindern.

Fazit

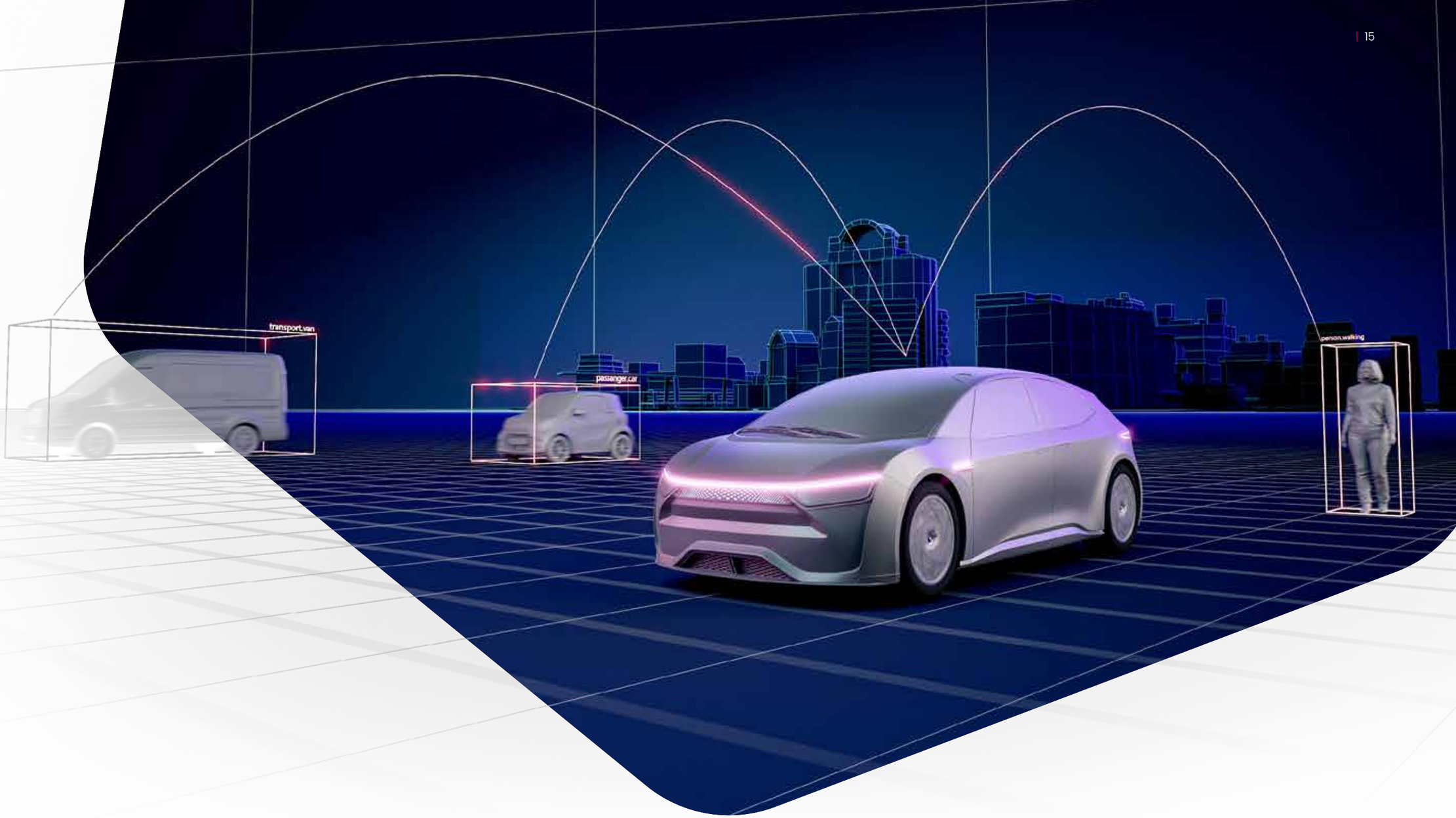
FEV.io bietet einen ganzheitlichen Cybersecurity-Ansatz in der Automobilindustrie, der auf umfassendem Fachwissen des Unternehmens über den gesamten Lebenszyklus der Cybersicherheit aufbaut. Diese Expertise, gepaart mit einer systematischen Methodik und innovativen Entwicklungen, stellt sicher, dass zukünftige Fahrzeuge nicht nur den Vorschriften entsprechen, sondern auch optimal gegen Cybersecurity-Bedrohungen gerüstet sind.

VON

Jagannath Tiwari,
tiwari_j@fev.com

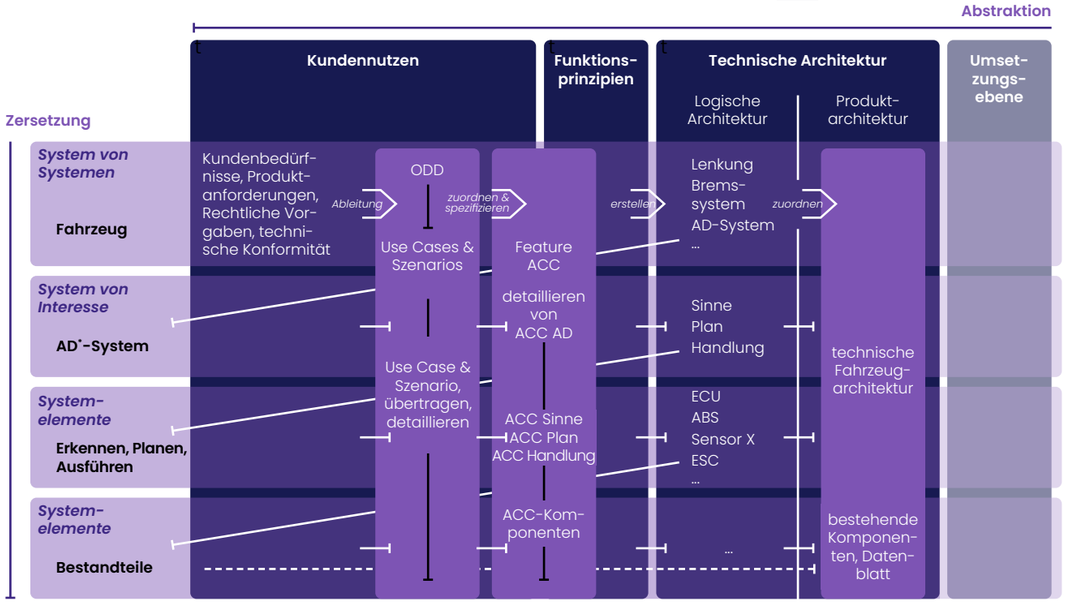
Yuri Gil Dantas,
dantas@fev.io

Matthias Rehberger,
rehberger@fev.io



#2
Beschleunigung homologationsrelevanter ***Softwareupdates***

Der Umfang rein softwarebasierter Funktionen im Fahrzeug nimmt spürbar zu. Das führt zu einem wachsenden Bedarf an Aktualisierungen und Erweiterungen von Funktionen. Dies betrifft auch softwaredefinierte Funktionen, die das Fahrzeug-Typgenehmigungsverfahren betreffen. Dadurch steht der Homologationsprozess vor neuen Herausforderungen, die sich aus der signifikanten Reduzierung der heute hohen Zeit- und Kostenaufwände für die Durchführung vor allem sicherheitskritischer Softwareaktualisierungen ergeben. Im Folgenden wird ein virtuell durchgeführter Entwicklungs- und Validierungsansatz vorgestellt, der konkret homologationsrelevante Softwareaktualisierungen ermöglicht.



1.
FEV.io CUBE Ansatz für modellbasiertes Systems- und Software-Engineering.

* AD = Autonomous Driving, automatisiertes Fahren

Gebündelte Kompetenzen

FEV.io hat sich mit den Unternehmen Kontrol, dSPACE, TÜV SÜD, Microsoft Deutschland, T-Systems und Berylls zusammengeschlossen, um ein Konzept für ein softwarebasiertes virtuelles Homologationsverfahren zu entwickeln. Hierbei sollen umfangreiche OTA- (Over The Air-)Fahrzeugaktualisierungen über Mobilfunk zum Einsatz kommen. Der Prozess der virtuellen Validierung soll sich künftig industrieweit etablieren und ein anerkannter Nachweis für die virtuelle Homologation von Software-Updates werden.

Besagter Nachweis erfordert u. a. eine lückenlose Rückverfolgbarkeit der gesetzlichen Anforderungen und des Funktionsdesigns. Hinzu kommen die implementierten Softwarequellcodes und die abgeleiteten Testfällen für jedes Software-Update.

Dieser volldigitalisierte Zyklus namens „Digital-Loop" bietet Fahrzeugherstellern und Zulassungsbehörden entscheidende Vorteile, da der Umfang der in der realen Umgebung benötigen Testaktivitäten durch die neue Lösung signifikant reduziert und damit sowohl Zeit als auch Kosten bei der Typgenehmigung während des gesamten Lebenszyklus eines Fahrzeugs eingespart werden können.

Die Grundlage dieses Ansatzes besteht in der Simulation realer Verkehrsszenarien mit modernster Simulationstechnik, um die erforderliche Genauigkeit und Zuverlässigkeit der virtuellen Umgebung für die Prüfung, Validierung und Zulassung zu erzielen. Diese virtuelle Simulationsumgebung ist ein umfassendes digitales Abbild der realen Welt, welches auf hochdetaillierten 3D-Modellen von Straßen, Fahrzeugen, Fußgängern, Wetterbedingungen und anderen Faktoren basiert. Die Fahrzeugsysteme werden mit diesen Simulationen stimuliert und daraufhin ihre Fahrentscheidungen bewertet.

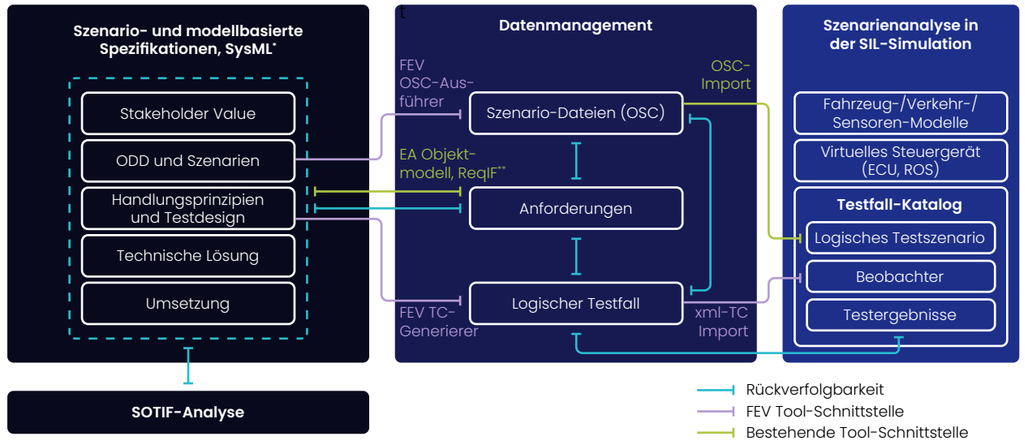
Funktionsorientierter Ansatz

Zur Genehmigung von SW-Updates, die für die Homologation relevant sind und unter die Software-Update-Management-(SUMS-)Verordnung fallen, ist es entscheidend, dass die Rückverfolgbarkeit über sämtliche Ebenen der Zerlegung und Abstraktion erfolgt. Dies betrifft alle Systeme und Teilkomponenten sowie den gesamten Entwicklungs- und Lebenszyklus des Produkts. Diese Rückverfolgbarkeit kann zeitlichen und räumlichen Veränderungen unterliegen. Der „Digital-Loop"-Ansatz zielt darauf ab, die Anforderungen der technischen Prüforganisation an eine klare und eindeutige Nachvollziehbarkeit der Auswirkungen von Softwareaktualisierungen auf bereits zugelassene Systeme zu erfüllen. Dabei werden die Prinzipien des Model-Based Systems Engineering (MBSE) angewendet. Die „Compositional Unified System-Based Engineering“ (CUBE) Methodik von FEV.io dient als grundlegender Rahmen für die Anforderungsspezifikation, das Produktdesign und die Implementierungsphase. Der funktionsgetriebene Ansatz von CUBE zeichnet sich durch eine lösungsneutrale Sichtweise aus, die den Anforderungen sowohl der aktuellen als auch zukünftigen softwaregetriebenen Produktentwicklung (Abb. 1) gerecht wird. Dieser Ansatz kann in der Entwicklung sämtlicher Funktionsbereiche innerhalb der Fahrzeugarchitektur angewendet werden. Ein Beispiel hierfür ist die Entwicklung einer ADAS-Funktion, bei der zusätzlich der szenariobasierte Entwicklungsansatz verwendet wird.

Um einen szenariobasierten Systementwurf mit Hilfe von MBSE zu realisieren, müssen neben den klassischen Anforderungs- und Use-Case-Spezifikationen auch der vorgesehene zulässige Betriebsbereich (Operational Design Domain, ODD) sowie die relevanten Szenarien der zu entwickelnden ADAS-Funktion in das Spezifikationsmodell integriert werden. Für dessen Modellierung werden erweiterte Profile von Modellierungssprachen wie UML oder SysML verwendet, die zusätzliche Diagramme und Modellelemente umfassen. Dabei müssen die modellierten Szenarien eine maschinenlesbare Definition der zeitabhängigen Interaktion zwischen dem gesteuerten Fahrzeug und seiner Umgebung enthalten. Dies umfasst sowohl logische Szenarien mit Beschreibungen der Parameterräume im Zustandsraum als auch konkrete Szenarien, die repräsentativ für diesen Zustandsraum sind.

Bei der Erstellung des Spezifikationsmodells unter Anwendung des CUBE-Ansatzes werden alle Modellkomponenten, beginnend mit der obersten Dekompositionsebene über alle Abstraktionsebenen hinweg in Relation gesetzt und spezifiziert. Dieser Vorgang wird systematisch für die nachfolgenden Dekompositionsebenen wiederholt, bis hinunter zur Ebene einzelner Komponenten (Steuergeräte, ECU). Das Ergebnis ist eine erweiterte System- und Softwarespezifikation, die eine detaillierte Rückverfolgbarkeit für alle Systeme und Teilsysteme ermöglicht. Dies geht über die Anforderungen von Reifegradmodellen wie Automotive SPICE hinaus. Durch die Verknüpfung von Anforderungen und Szenarien in einem einzigen Modell mithilfe von Werkzeugen kann die vollständige Rückverfolgbarkeit bis zur Softwareebene sichergestellt werden. Gleichzeitig können die Auswirkungen von Softwareaktualisierungen oder neuen homologationsrelevanten Funktionen effizient analysiert werden. Dies bildet einen wesentlichen Bestandteil der Argumentation gegenüber technischen Prüforganisationen im Rahmen von virtuellen Fahrzeugtypzulassungsaktivitäten.

Zudem ermöglicht dieses umfassende Spezifikationsmodell die automatische Generierung der homologationsrelevanten Szenarien und maschinenlesbaren Testfälle einschließlich der Pass/Fail-Kriterien für die virtuelle Absicherung auf der Grundlage der formalisierten Szenariospezifikation und der Verhaltensdiagramme in CUBE. Dies ermöglicht nicht nur höchste Qualität der Testfälle, sondern auch beste Rückverfolgbarkeit zu den Anforderungen und gleichzeitig die Möglichkeit zur signifikanten Reduzierung des Validierungsaufwandes. Die Verwendung standardisierter Schnittstellen mit anderen Partnern der „Digital-Loop"-Arbeitsgruppe trägt zusätzlich zur kontinuierlichen Integration der Simulation in die Entwicklungsumgebung bei.



2.
Automatische Generierung von Verifikations- und Validierungsartefakten.

Simulation als Homologationsnachweis

Ein weiteres Hauptziel des „Digital-Loops" besteht darin, Simulation als einen Nachweis für die Zulassung innerhalb des Verifizierungs- und Validierungsprozesses zu etablieren. Hierfür bietet der Projektpartner dSPACE eine Cloud-basierte Simulations- und Validierungslösung an, die Datenwiedergabe und szenarienbasierte Tests ermöglicht. Darüber hinaus können alle zuvor genannten Entwicklungsartefakte bis hin zum virtuellen Steuergerät automatisiert in die Lösung integriert werden, einschließlich der relevanten Testszenarien und deren Akzeptanzkriterien.

Um eine effektive virtuelle Validierung zu ermöglichen, müssen Messdaten aus realen Fahrversuchen in die virtuelle Validierung eingebracht werden. Dies geschieht durch die Analyse der Messdaten vor der eigentlichen Simulation, um relevante Situationen zu identifizieren und einen Katalog realistischer Szenarien zu erstellen. Selten auftretende Situationen (Edge Cases, Grenzfälle) können in der Simulation präzise reproduziert werden. Zudem können logische Simulationsszenarien parametrisiert werden, um neue Varianten und zusätzliche Testfälle zu generieren und somit neue Grenzfälle aufzudecken. Dieser datengetriebene Prozess ist entscheidend sowohl für die Identifizierung relevanter Situationen als auch für die Absicherung der Simulationsmodelle. Durch die Anpassung der Umwelteinflüsse und äußeren Randbedingungen können weitere relevante Situationen erfasst werden. Dieser Ansatz erweitert und verbessert den traditionellen Homologationsprozess, indem er den notwendigen Nachweis für die Abdeckung der relevanten Test- und Validierungsanforderungen unterstützt.

Um die Simulation als Akzeptanzkriterium zu nutzen, müssen die Simulationsmodelle als eigenständige Engineering-Artefakte verifiziert und validiert werden. Hierbei werden die physikalischen Messgrößen aus dem simulierten Szenario mit den tatsächlich gemessenen Größen verglichen, um eventuelle Anpassungen im Modell vorzunehmen. Ein fortlaufender Abgleich und die entsprechende Dokumentation sind entscheidende Nachweise für den virtuellen Homologationsprozess. Dieser kann beschleunigt werden, indem die Ergebnisse der Testdurchführung aller relevanten Szenarien und die Überwachung der Akzeptanzkriterien innerhalb der Simulation in einem digitalen Bericht dokumentiert werden.

Erfahren Sie hier mehr zu Digital Loop

VON
Sebastien Christians,
christiaens@fev.io
Elmar Börner,
boerner@fev.com

#3
Testzentrum in Marokko: Ganzjährige Entwicklungs- und Erprobungsarbeit im Bereich *ADAS/AD*

FEV betreibt gemeinsam mit einem Joint Venture-Partner das erste Automobil-Testzentrum des afrikanischen Kontinents. Im marokkanischen Oued Zem nahe Casablanca bietet der international anerkannte Innovationstreiber seinen Kunden nahezu ganzjährig hochattraktive Bedingungen für die Fahrzeugentwicklung und -erprobung.

Das Moroccan Mobility & Automotive Test Center (MMAC) in Oued Zem liegt auf 850 Metern Höhe im marokkanischen Atlas-Vorgebirge. Das Gelände mit insgesamt 500 Hektar Fläche umfasst ein weitläufiges, komplett neu gebautes Testgelände für Pkw und Nutzfahrzeuge, das auf insgesamt 14 Teil- und Einzelstrecken unterschiedlichste Erprobungsfahrten ermöglicht.

Im Bereich ADAS/AD bietet FEV in optimaler Umgebung vor Ort in drei Funktionsbereichen sein Validierungs-Know-how an.

Longitudinale und laterale Funktionen (Driver Assistance: ADAS Road Driving Features) L0 bis L2

- Automatic Emergency Braking (AEB)
- Adaptive Cruise Control (ACC)
- Automatic Lane Change (ALC)
- Blind Spot Detection (BSD)
- Cross Traffic Alert (CTA)
- Front Collision Warning (FCW)
- Lane Centering Control (LCC)
- Lane Departure Prevention (LDP)
- Lane Keep Assist (LKA)

Hochautomatisierte Funktionen (AD Driving Features) L2+ bis L4

- Traffic Jam Pilot/Chauffeur bis 60 km/h
- Highway Pilot/Chauffeur bis 130 km/h

Parkfunktionen (ADAS/AD Parking Features) L2+ bis L4

- 360° Surround View
- Parking Assist
- Parking Pilot/Remote Parking
- Automated Valet Parking Type 1

[ADAS/AD Testzentrum]

Weitere Informationen zum Testzentrum in Qued Zem, Marokko

#4
Innovationsbeschleuniger: ***Software-Engineering @ FEV.io India***

1.
Um Innovationen zu beschleunigen, ist der Aufbau von robusten Software-Engineering-Teams weltweit unabdingbar. FEV nutzt sein umfangreiches Fachwissen in den Bereichen Software und Elektronik, ergänzt um fundierte Kenntnisse in allen übrigen Anwendungsbereichen der Fahrzeugtechnik, die für intelligente Mobilitätslösungen entscheidend sind. So bietet FEV seinen Kunden weltweit erstklassige Ingenieurdienstleistungen. Gemeinsam verfolgen wir das Ziel, Menschen auf der ganzen Welt zu verbinden und zu mobilisieren.

Der Mobilitätssektor befindet sich derzeit inmitten des wahrscheinlich revolutionärsten Umbruchs seit Erfindung des Automobils. Zukünftig werden neben nachhaltigen Antriebstechnologien vor allen Dingen softwarebasierte Innovationen und Verbesserungen über den Erfolg neuer Mobilitätslösungen entscheiden. Der Wandel des Fahrzeugs vom reinen Fortbewegungsmittel hin zum digitalen Ökosystem und wichtigem Raum des täglichen Lebens hat ein grundlegendes Umdenken hinsichtlich der Anforderungen an die Fahrzeugfunktionalitäten und dementsprechend in der Konstruktion und Entwicklung der Fahrzeuge von morgen angestoßen.

Der Trend zur Digitalisierung in der Mobilität wird durch unterschiedliche Faktoren verstärkt und beschleunigt. Insbesondere das veränderte Verbraucherverhalten, verschärfte gesetzliche Anforderungen im Hinblick auf Nachhaltigkeit sowie die kontinuierliche Verfügbarkeit neuer Technologien treiben die Evolution maßgeblich voran. Eine Schlüsselrolle in diesem Transformationsprozess nehmen Softwarelösungen ein, sei es in vernetzten Flotten oder in autonom agierenden Fahrzeugen. Sie spielen eine führende Rolle bei der Verbesserung von Sicherheit, Effizienz und Leistung in der Mobilität. Die damit einhergehende Nachfrage nach fortschrittlichen und innovativen Lösungen ist dementsprechend enorm hoch und wird voraussichtlich weiter steigen. Zeitgleich hat die Digitalisierung Einfluss auf die Qualifikationen in der Fahrzeugentwicklung: Ergänzend zu den klassischen Professionen der Fahrzeugtechnik wächst der Bedarf an qualifizierten Softwareingenieurinnen und -ingenieuren.

»FEV entwickelt sichere und nachhaltige Mobilitätslösungen, die das Leben der Menschen auf der ganzen Welt verbessern.«

Als weltweit anerkannter Experte in der Entwicklung von Mobilitäts- und Fahrzeugtechnologien hat FEV die strategische Bedeutung von Software für die zukünftige Gestaltung der Mobilität erkannt. Das signifikante globale Wachstum sowohl der Marke FEV.io als auch der Softwareentwicklung innerhalb des gesamten Unternehmens trägt bereits aktiv zur Förderung des Transformationsprozesses der Mobilitätsbranche bei. Als Reaktion auf diese Entwicklung erweitert FEV gezielt seine Ressourcen in diesem essenziellen Bereich, um den bevorstehenden Herausforderungen effektiv begegnen zu können.

Mit Etablierung der Marke FEV.io hat das Unternehmen die Herausforderung der steigenden Anforderungen und dem rasanten Entwicklungstempo im Bereich der intelligenten Mobilität erfolgreich angenommen. Das umfassende Leistungsportfolio erstreckt sich über alle relevanten Bereiche: Sowohl in der Systementwicklung (Systems Engineering), der Funktionalen Sicherheit & Cybersecurity, dem Autonomen Fahren (ADAS/AD) aber ebenso in den Themenfeldern E-Cockpit & Konnektivität, SW & EE Plattformen/Integration bietet FEV.io umfangreiches und tiefgehendes Know-how.

Die Maxime des internationalen FEV.io Teams mit seinen mehr als 1.400 Software-Experten lautet dabei, sichere und nachhaltige Mobilitätslösungen zu entwickeln, die das Leben der Menschen auf der ganzen Welt verbessern.

In der bisherigen Wachstums- und Erfolgsgeschichte von FEV.io spielt das Team von FEV India eine entscheidende Rolle. Das Zentrum in Pune gilt als Software-Powerhouse innerhalb des Unternehmens und besteht aus über 600 hochmotivierten Expertinnen und Experten. Dieses Team hat bereits mehrfach seine Fähigkeit unter Beweis gestellt, innovative und maßgeschneiderte Softwarelösungen zu entwickeln und zu liefern. So hat FEV India im Jahr 2023 mit der Anmeldung von 27 Erfindungen in verschiedenen Bereichen wichtige Meilensteine gesetzt und seine Position als globales Exzellenzzentrum in den Bereichen Software Defined Vehicle, Cybersecurity, E-Cockpit & Konnektivität und technische Analyse gefestigt. Daher blickt das indische Team in dieser entscheidenden Phase des Transformationsprozesses mit Stolz auf seine Rolle als Wissenspartner in Industriepartnerschaften mit international bekannten Kunden.

Durch die Fokussierung auf das Vorantreiben von Innovationen, die Nutzung der indischen Expertise im Software-Engineering und den Zugang zu einem umfangreichen Pool talentierter Softwareentwickler ist FEV optimal positioniert, um den stetig wachsenden Anforderungen der Mobilitätsbranche erfolgreich zu begegnen. Indien wird als anerkanntes Zentrum für technologische Innovationen von FEV als ideale Option betrachtet, um die eigene Softwarekompetenz auch künftig weiter auszubauen.

2.
Die Ernennung von Mayank Agochiya zum Vorsitzenden der Geschäftsführung von FEV Asia ist ein bedeutsamer Schritt und fügt sich nahtlos in das Engagement von FEV für Innovation und Wachstum speziell im Bereich der Softwareentwicklung ein. Seine vielseitige Erfahrung und sein tiefes Verständnis der Mobilitäts- und Energiewelt werden FEV zu neuen Erfolgen in der dynamischen Landschaft von Innovation und Technologie verhelfen.

#5 *Zukunftsfähige Mobilität mit FEV und SELFY:* Resilienz, Kooperation, Vernetzung und Automatisierung

Die rasante Entwicklung in den Bereichen Vernetzung und Automatisierung hat auch in der Mobilität Einzug gehalten. Das Ziel von vernetzter und automatisierter Mobilität (Cooperative Connected Automated Mobility, CCAM) ist es, Transportsysteme durch integrierte Netzwerke von Fahrzeugen, Fußgängern, Straßeninfrastrukturen, Fahrzeug-Infrastruktur-Schnittstelle (engl. Roadside Units, RSUs) und Cloud-Diensten zu verbessern. Mit zunehmender Vernetzung entstehen jedoch auch neue digitale Bedrohungen und das Ausmaß möglicher Cyber-Angriffe nimmt erheblich zu. Eine weitere Herausforderung besteht darin, Daten aus Fahrzeugen, Infrastruktur und Cloud-Diensten zusammenzuführen und Künstliche Intelligenz (KI) auf diese Daten anzuwenden, um ein entsprechendes Situationsbewusstsein zu schaffen.

Motiviert durch diese Herausforderungen wurde 2022 das Projekt SELFY (SELF Assessment, Protection, Healing Tools for a TrustworthY and Resilient CCAM) ins Leben gerufen. Im Rahmen des europäischen Forschungs- und Innovationsprogramms Horizon 2020 zielt das dreijährige Projekt darauf ab, Werkzeuge (nachfolgend Tools) zu entwickeln, die die Widerstandsfähigkeit des CCAM-Ökosystems gegenüber Cyber-Bedrohungen und -angriffen erhöht.

FEV ist innerhalb des Konsortiums zuständig für:

- die Einrichtung der Systemarchitektur
- den Aufbau eines KI-Systems zur kontinuierlichen Selbstbewertung und Diagnose sowie zur Erkennung anomaler Situationen
- die Entwicklung von Sicherheitsmethoden um die Kommunikationspfade in CCAM vor Cyberangriffen zu schützen
- die Entwicklung von Maßnahmen, um Integrität, Vertraulichkeit und Authentizität auf den Kommunikationskanälen zu gewährleisten
- die Durchführung von Verifikations-und Validierungstests sowie Funktionsprüfungen

Die SELFY-Tools sollen eine umfassende globale Lösung bieten, indem Schutz-, Reaktions- und Wiederherstellungsmaßnahmen sowohl lokal als auch global koordiniert werden. Dieser Artikel bietet einen Überblick über die wichtigsten Makro-Tools von SELFY und beschreibt drei übergeordnete Anwendungsfälle, die im Projekt definiert wurden. Darüber hinaus werden die Tools „Situationsbewertungsmodul" (Situational Assessment Module, SAM) und „Sicheres Over-The-Air Software Update" (Secure Over-The-Air Software Update, SOTA) erläutert, die aktuell von FEV entwickelt werden.

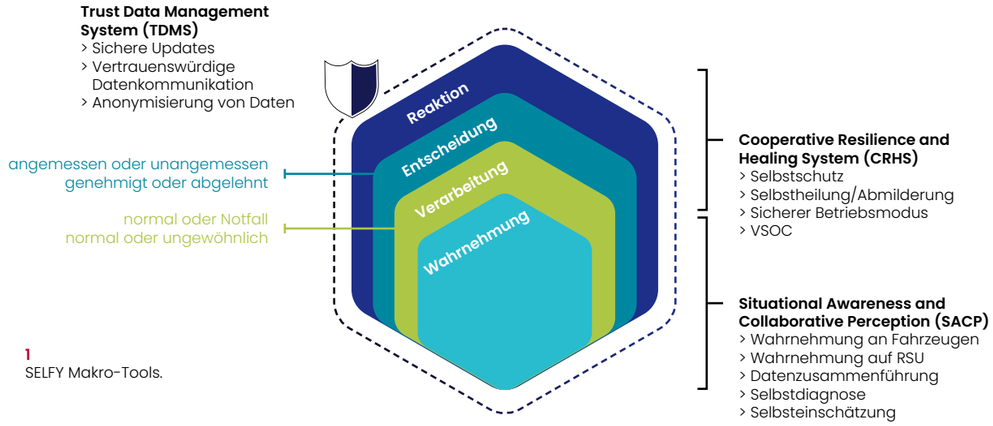
SELFY Makro-Tools

Die SELFY-Toolbox bewertet fortlaufend die Stabilität sowie Widerstandsfähigkeit und profitiert dabei von einem Situationsbewusstsein, das durch kooperative Wahrnehmung erreicht wird. Sie bietet verschiedene kooperative Resilienz-Dienste, um Risikosituationen zu bewältigen, indem sie Daten innerhalb eines vertrauenswürdigen kollaborativen Rahmens sammelt und austauscht. Die wichtigsten Technologien der SELFY-Toolbox und die drei Hauptwerkzeuge, in die diese Technologien unterteilt sind, werden nachfolgend veranschaulicht (Abb. 1).

Situationsbewusstsein und kollaborative Wahrnehmung (Situational Awareness and Collaborative Perception, SACP)
Die SACP-Box beinhaltet eine Vielzahl von Tools, die entwickelt wurden, um ein umfassendes Verständnis der CCAM-Systemumgebung zu ermöglichen, einschließlich verschiedener Assets oder Geräte im Fahrzeug und in der RSU. Um die Umgebung des Fahrzeugs zu interpretieren, besteht die SACP aus separaten Modulen, die die Wahrnehmung des Fahrzeugs und der RSU bereitstellen. Ein weiteres Modul kann diese beiden Wahrnehmungen zusammenführen, während weitere Module Anomalien sowohl am Fahrzeug als auch an der RSU erkennen können.

Kooperatives Resilienz- und Heilungssystem (Cooperative Resilience and Healing System CRHS)
Die CRHS-Box enthält Tools, die Selbstschutzmaßnahmen einleiten, um auf gefährdende Szenarien zu reagieren. Diese können Assets, Fahrzeuge, Abläufe oder das System betreffen. Eine Reaktion kann die Einleitung eines sicheren Betriebsmodus für das Fahrzeug sein. In diesem Fall ist das Tool für die Ermittlung, Ausführung und Bewertung des Status des ausgewählten sicheren Betriebsmodus verantwortlich, der für die erkannte Situation geeignet ist. Resilienzmaßnahmen können lokal oder in Zusammenarbeit mit anderen Knotenpunkten innerhalb des CCAM durchgeführt werden, was eine globale Entscheidungsfindung ermöglicht. Das Vehicle Security Operations Center (VSOC) innerhalb des CRHS verfügt über diese globale Entscheidungsfähigkeit.

Vertrauensdatenmanagement-System (Trust Data Management System, TDMS)
Die TDMS-Box umfasst alle Tools, die zum Aufbau einer sicheren und vertrauenswürdigen Umgebung für Daten in einem kollaborativen und kooperativen Kontext gedacht sind. Dies gilt sowohl für Infrastruktur und Assets als auch für Personendaten, etwa von Fahrern oder Fußgängern. Ziel ist es hierbei, die Integrität verschiedener Softwarekomponenten sicherzustellen, den Datenschutz zu berücksichtigen und sichere Software-Updates für vernetzte und automatisierte Fahrzeuge zu verwalten.



1
SELFY Makro-Tools.

Drei übergeordnete Anwendungsfälle von SELFY

Die SELFY-Toolbox soll in drei verschiedenen Makroszenarien validiert werden, die drei Validierungsumgebungen von SELFY entsprechen. Dies sind neben der realen Welt die Labor-/Hardware-In-the-Loop-(HIL-)Validierung und die Simulationsvalidierung.

1

Resiliente kooperative Mechanismen für die Sicherheit gefährdeter Verkehrsteilnehmer (Vulnerable Road User, VRU)
Die zunehmende Zahl automatisierter Fahrzeuge erfordert eine Verbesserung der Sicherheit von VRUs wie Fußgängern und Radfahrern und zu diesem Zweck ein intelligentes Zusammenwirken zwischen automatisierten Fahrzeugen, von durch Menschen gesteuerten Fahrzeugen und VRUs selbst. Resiliente kooperative Mechanismen für das VRU-Sicherheitsszenario bestehen aus Wahrnehmung, Situationsbewusstsein, Kommunikation und Entscheidungsfindung, unterstützt durch Risikobewertung.

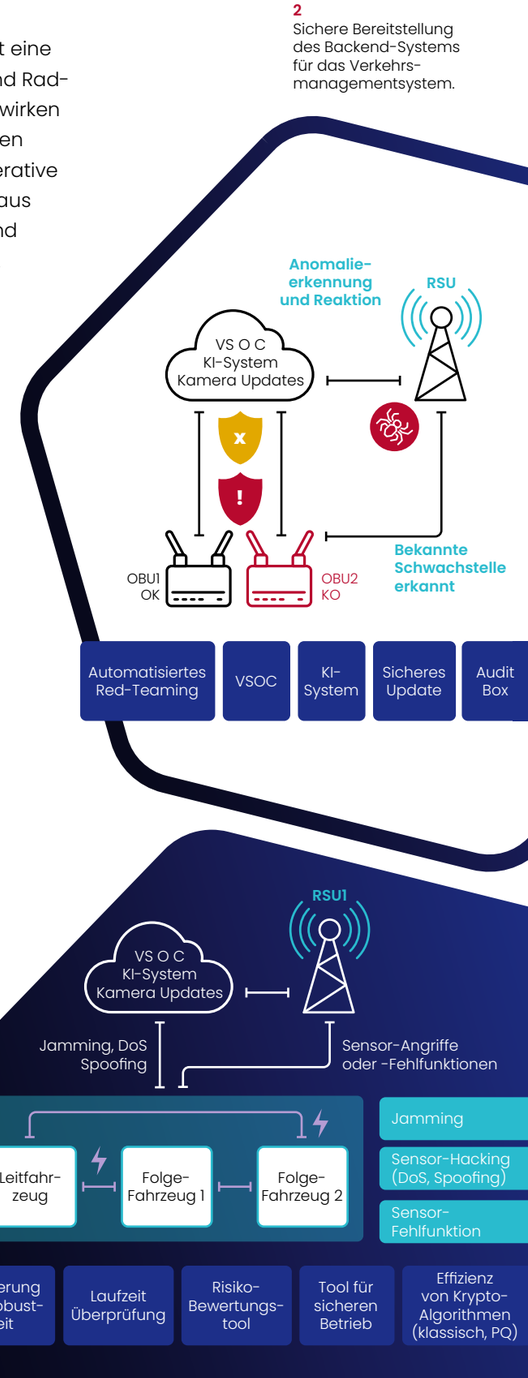
2

Sichere Bereitstellung des Backend-Systems für das Verkehrsmanagementsystem
Das CCAM-Ökosystem erfordert sichere und robuste Remote-Datenverbindungen zu Cloud-Servern. In Zukunft wird wahrscheinlich jeder Fahrzeughersteller (Original Equipment Manufacturer, OEM) VSOCs einrichten müssen, um die Cybersicherheit seiner Fahrzeuge zu überwachen und Sicherheitsvorfälle, Anomalien und Gefahren zu melden.

Verkehrsmanagementsysteme oder OEMs müssen die Möglichkeit haben, ihre eigenen Parameter und Vertrauensniveaus für das VSOC festzulegen. Diese können von Straßen- und Fahrzeugzustand, zulässigen Manövern, Reaktionen und beeinträchtigten Modi abhängen. Das VSOC verfügt über eine Reihe von Tools zur Prüfung des Systems sowie über fortschrittliche Algorithmen zur Erkennung von Bedrohungen und Bereitstellung von Reaktionen (Abb. 2).

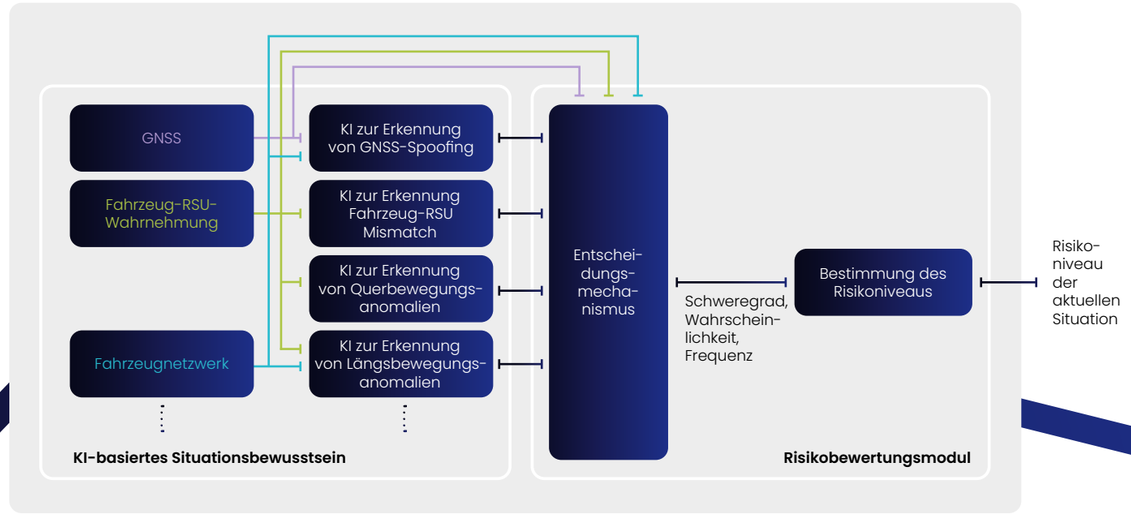
3

Steigerung der Robustheit eines Platoons
Platooning bezeichnet eine Technologie, die es mehreren automatisierten Fahrzeugen ermöglicht, bei hoher Geschwindigkeit sicher zusammen zu fahren. Dabei ist es unerlässlich, eine zuverlässige Kommunikationsverbindung zwischen allen Fahrzeugen des Platoons sicherzustellen.
Die SELFY-Tools zielen darauf ab, diese Verbindung zu verbessern und potenzielle Risiken zu mindern (Abb. 3).



3
Steigerung der Robustheit eines Platoons.

4
Situationsbewertungsmodul.



Situationsbewertungsmodul (SAM)

Das Situationsbewertungsmodul (Situational Assessment Module, SAM) soll die Fähigkeit KI-basierter Systeme verbessern, Anomalien zu erkennen und unter verschiedenen Betriebsbedingungen Entscheidungen zu treffen. Unter Verwendung fortschrittlicher KI-basierter Techniken vergleicht das SAM fusionierte Daten von RSU und Bordfahrzeugsensoren mit den CAN-Nachrichten des Fahrzeugs (Abb. 4). Basierend auf einer erkannten Anomalie bestimmt SAM den Risikograd der aktuellen Situation, die beispielsweise durch einen Missbrauch oder eine Fehlfunktion aufgetreten ist. Um dieses Ziel zu erreichen, wurden vier verschiedene KI-Modelle entwickelt. Jedes Modell übermittelt Daten an einen Entscheidungsmechanismus, der einen sicheren Betriebsmodus für das Fahrzeug auswählt.

Die primär untersuchte Anomalie ist das Phänomen des Global Navigation Satellite System (GNSS) Loss-Spoofing. Basierend auf einer Entfernungsschätzung wird erkannt, ob GNSS-Daten während des Fahrzeugbetriebs nicht plausibel oder nicht mehr verfügbar sind. Eine zweite Anomalie, RSU-Vehicle Mismatch, liegt vor, wenn vom Fahrzeug erhaltene Daten und RSU-Daten inkonsistent zueinander sind. Die Erkennung solcher Nichtübereinstimmungen überführt das Fahrzeug in einen anomalen Zustand. Weitere Anomalien umfassen unerwartete Änderungen der Beschleunigung, Verzögerung und Lenkung während der Fahrt unter Berücksichtigung von Faktoren wie Verkehrsinteraktionen und normalen Geschwindigkeiten des Fahrzeugs.

Während der Betriebsphase von KI-Modellen werden erkannte Anomalien an den Entscheidungsmechanismus übermittelt. Berechnete Häufigkeits-, Wahrscheinlichkeits- und Schweregrade fließen in die Interpretation der Situation ein und werden anhand einer vorab festgelegten regelbasierten Entscheidungstabelle ausgewertet. Das Resultat ist die Angabe eines Risikoniveaus, welches für weitere Entscheidungsprozesse zur Verfügung steht.

Sicheres Over-The-Air-Software-Update

Ein Anwendungsfall veranschaulicht die Notwendigkeit der Erkennung von Schwachstellen veralteter Software und der Bereitstellung von Software-Updates und Fehlerbehebungen über einen sicheren Aktualisierungsmechanismus. In diesem Szenario erkennt die RSU eine Schwachstelle beziehungsweise einen Fehler im Fahrzeug und informiert alle umliegenden Fahrzeuge. Ein verdächtiges Verhalten wurde von dem vorausfahrenden Fahrzeug erkannt und als Ursache eine kompromittierte oder veraltete Softwareversion identifiziert. Als Abhilfemaßnahme wird ein Software-Update auf das Fahrzeug übertragen.

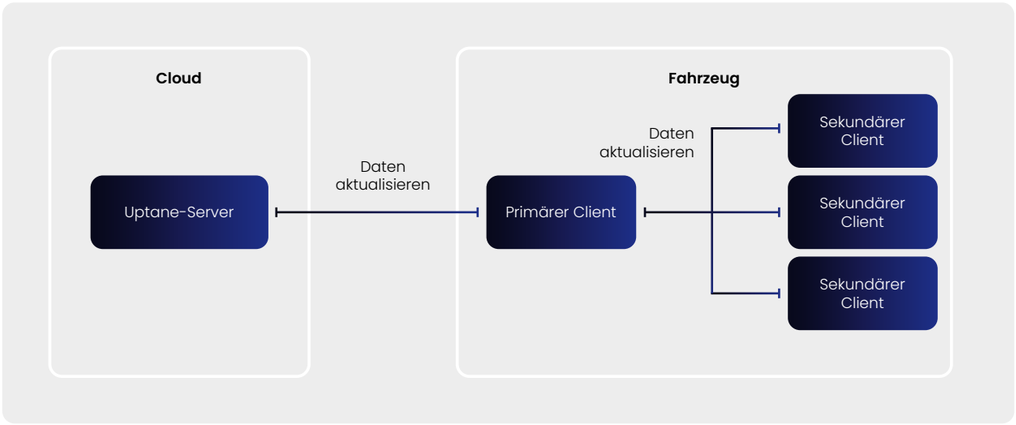
In dem Anwendungsfall wird das Software-Update mit einem SOTA-Tool durchgeführt, das Teil des TDMS-Makrotools ist. Das Hauptziel dieses Tools ist die sichere und effiziente Bereitstellung von Software-Updates für die elektronischen Steuergeräte (Electronic Control Units, ECUs) des Fahrzeugs aus der Ferne. Diese Fähigkeit ist von entscheidender Bedeutung für die Aufrechterhaltung oder Verbesserung der Fahrzeugfunktionen. Es stellt sicher, dass die neuesten Cybersicherheitsmaßnahmen schnell umgesetzt werden, Schwachstellen behoben und die Sicherheitsfunktionen des Fahrzeugs verbessert werden. Zeitintensive Vor-Ort-Besuche beim Händler sind dabei nicht notwendig.

Insbesondere für vernetzte und automatisierte Fahrzeuge wird der OTA-Softwareaktualisierungsprozess in den kommenden Jahren von großer Bedeutung sein und die Aktualisierung des Fahrzeugsoftwaresystems in der mobilen Welt beschleunigen.

»Sichere Updates sind durch Quantenfortschritte gefährdet. Das SELFY-Projekt steuert dem durch die Integration postquantenkryptografischer Algorithmen in das SOTA-Framework entgegen.«

Die Sicherheit des OTA-Update-Prozesses ist von entscheidender Bedeutung, da er Zugriff auf das interne Kommunikationssystem des Fahrzeugs erfordert und zusätzliche Angriffspunkte aus der Ferne auf alle Steuergeräte bietet, die über die OTA-Funktion verfügen. Um diese Sicherheit zu gewährleisten, veröffentlichte die Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) im Jahr 2021 die Verordnung R156, die die Cybersicherheit von Software-Updates und des Software-Update-Management-Systems für Fahrzeuge fordert. Im Rahmen des SELFY-Projekts wird besonderes Augenmerk auf die Sicherheit des OTA-Software-Update-Prozesses gelegt. Der Kern des SOTA-Tools basiert auf dem Uptane-Framework (Abb. 5).

- **Uptane-Server:** Diese serverseitige Komponente ist dafür verantwortlich, sichere Software-Updates vorzubereiten, sie kryptografisch zu signieren und an entsprechende Fahrzeuge zu verteilen. Es ist der Ausgangspunkt für den sicheren Update-Lebenszyklus.
- **Primärer Client:** Der in das Fahrzeug eingebettete primäre Client fungiert als vermittelndes Steuergerät und empfängt Aktualisierungen vom Uptane-Server. Es überprüft die Signaturen und die Integrität der Updates, bevor es sie an die sekundären Clients verteilt.
- **Sekundäre Clients:** Diese fahrzeuginternen Komponenten erhalten Updates vom primären Client. Jeder sekundäre Client ist für die unabhängige Überprüfung und Installation dieser Updates verantwortlich, um seine spezifische Fahrzeugfunktion zu verwalten.



5
SOTA-Architektur.

Die OTA-Updates erfordern langfristige Sicherheit. Um Schwachstellen entgegenzuwirken, die lange nach der Produktion des Fahrzeugs entdeckt werden, muss der OTA-Update-Mechanismus vor zukünftigen Bedrohungen geschützt werden. Das Aufkommen von Quantencomputern stellt jedoch die bestehenden kryptografischen Praktiken in Fahrzeugen vor erhebliche Herausforderungen. Aktuelle Fahrzeuge sind für sichere Updates auf die Kryptografie mit öffentlichen Schlüsseln angewiesen. Während diese Methoden Integrität und Authentizität gewährleisten, sind sie durch Quantenfortschritte gefährdet. Um auch auf dieses Risiko vorbereitet zu sein, erfolgen im SELFY-Projekt Forschungsarbeiten an der Integration postquantenkryptografischer Algorithmen in das SOTA-Framework.

Haftungsausschluss
Diese Forschung wurde von der Europäischen Union im Rahmen des Forschungs- und Innovationsprogramms Horizon Europe im Rahmen der Fördervereinbarung Nr. 101069748 – SELFY-Projekt – finanziert. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder der Europäischen Exekutivagentur für Klima, Infrastruktur und Umwelt (CINEA) wider. Weder die Europäische Union noch die Bewilligungsbehörde können hierfür haftbar gemacht werden.

Weitere Informationen zum SELFY Projekt

VON
Burcu Oezbay,
oezbay@fev.com
Dr. Miao Zhang,
zhang_m@fev.io
Dr. Mohamed Saied Mohamed,
mohamed_m@fev.io
Ali Eren,
eren_a@fev.com

Zusammenfassung und Ausblick

Die Vision des SELFY-Projekts besteht darin, der wichtigste europäische Anbieter einer agnostischen Toolbox für die Selbstverwaltung von Sicherheit und Belastbarkeit des CCAM-Ökosystems zu werden.

Im nächsten Schritt wird das SELFY-Projekt die Integration und Validierung der Toolbox in Simulation, HIL-Tests und einem realen Szenario fortsetzen, um eine ganzheitliche und nachhaltige Lösung für Sicherheit und Belastbarkeit für alle am CCAM-Ökosystem beteiligten Stakeholder wie OEMs, Zulieferer und Transportdienstleister bereitzustellen.

feel evolution

FEV.io

FEV test systems

FEV propulsion

FEV vehicle

FEV energy

FEV CONSULTING

fev.com

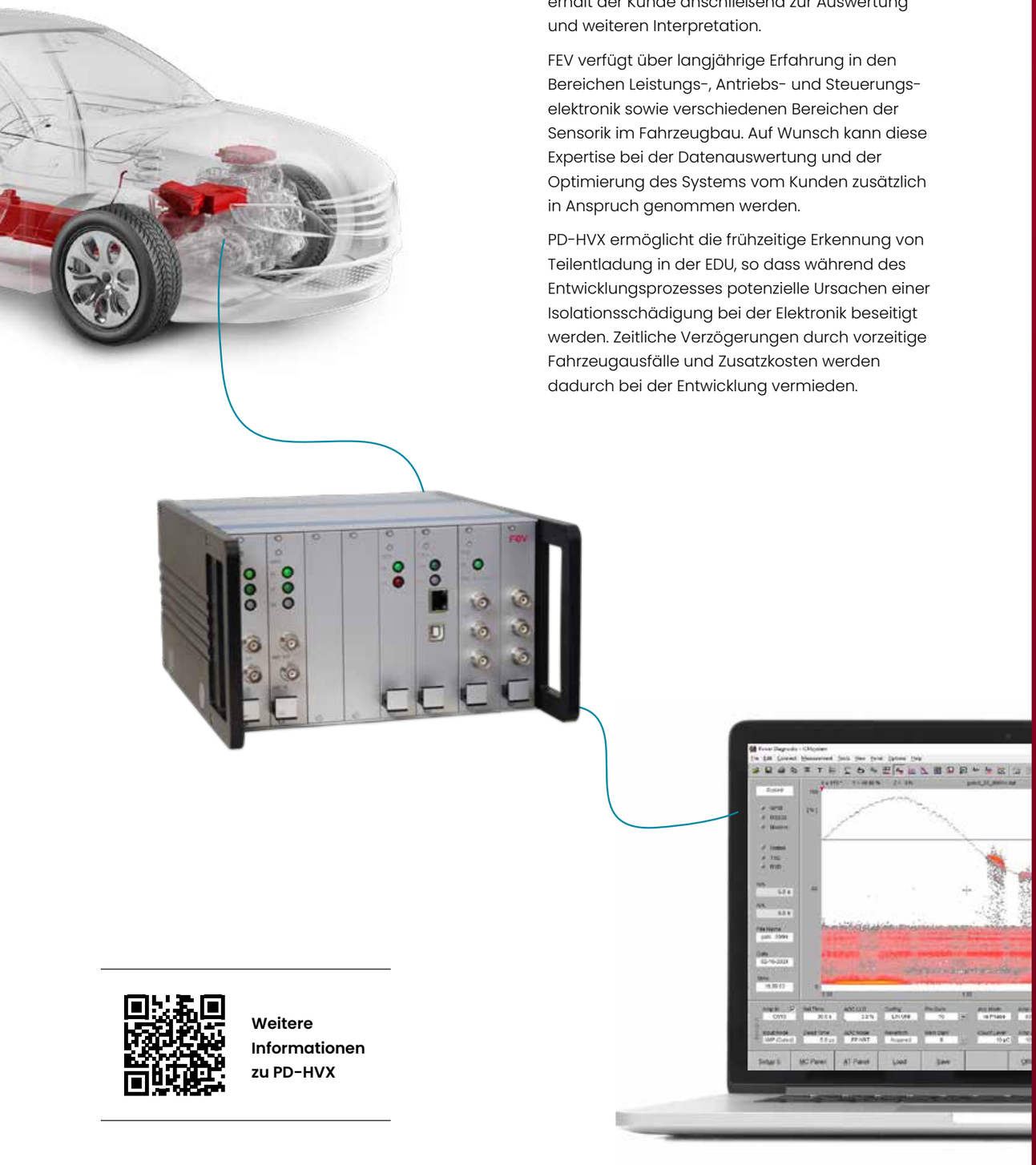
#6
Aufgespürt: Keine Chance für ***elektrische Teilentladung***

FEV hat mit PD-HVX („Partial Discharge-High Voltage X“) die weltweit erste Lösung zur Früherkennung und Prävention von Teilentladung in Hochvolt-Fahrzeugantrieben (Electric Drive Units, EDUs) entwickelt. Teilentladung (TE) kann in modernen EDUs Beschädigungen der Isolation verursachen, welche im ungünstigsten Fall einen Totalschaden des Fahrzeugs zur Folge haben. FEVs PD-HVX nutzt etablierte Messsysteme mit speziell entwickelten Sensoren, die in EDUs zur qualitativen Messerfassung eingesetzt werden. So können Kunden bereits während des Entwicklungsprozesses Teilentladung identifizieren und entsprechende Gegenmaßnahmen ergreifen.

Teilentladung ist ein lokal auftretender elektrischer Überschlag, der bei Spannungen größer 600 Volt entstehen kann. Ursächlich dafür sind kleinste Defekte oder Inhomogenitäten im Isolationsmaterial oder Verschmutzungen von Oberflächen. Sofern sie innerhalb einer EDU unentdeckt bleibt und wiederholt auftritt, führt TE zu einer fortschreitenden Schädigung der Isolierung und zu einem vorzeitigen Stillstand des Fahrzeuges.

PD-HVX misst mit Hilfe elektromagnetischer Frequenzanalyse, einer der präzisesten und verlässlichsten Messmethoden im Anwendungsbereich elektrischer Antriebe, die elektromagnetischen Felder rund um die zu analysierende Antriebseinheit. Aus den Messergebnissen leitet die innovative Lösung anschließend ab, ob während des Betriebs innerhalb der EDU Teilentladungen entstehen.

Im Bereich der elektrischen Anlagentechnik und Hochspannungs-Übertragungsnetze ist TE bereits seit langem bekannt. Entsprechende Tests sind dort gängige Praxis. Im Automobilsektor rückt das Phänomen hingegen erst mit der zunehmenden Verbreitung der 800-Volt-Batterien in den Fokus. Durch FEVs langjährige Kompetenz bei der Entwicklung von EDUs kann das Unternehmen seinen Kunden mit PD-HVX bereits heute eine Lösung zum Thema TE anbieten.



Dabei ist PD-HVX Teil eines ganzheitlichen Servicepakets für Fahrzeughersteller und Zulieferer. Die für den EDU-Betrieb optimierte Messtechnik filtert die antriebsrelevanten Störsignale heraus und erlaubt somit signifikant bessere Messergebnisse der TE. Die in den Tests gewonnenen Daten erhält der Kunde anschließend zur Auswertung und weiteren Interpretation.

FEV verfügt über langjährige Erfahrung in den Bereichen Leistungs-, Antriebs- und Steuerungselektronik sowie verschiedenen Bereichen der Sensorik im Fahrzeugbau. Auf Wunsch kann diese Expertise bei der Datenauswertung und der Optimierung des Systems vom Kunden zusätzlich in Anspruch genommen werden.

PD-HVX ermöglicht die frühzeitige Erkennung von Teilentladung in der EDU, so dass während des Entwicklungsprozesses potenzielle Ursachen einer Isolationsschädigung bei der Elektronik beseitigt werden. Zeitliche Verzögerungen durch vorzeitige Fahrzeugausfälle und Zusatzkosten werden dadurch bei der Entwicklung vermieden.

Weitere Informationen zu PD-HVX

Was macht FEVs Lösung PD-HVX so besonders?

PD-HVX ist die weltweit erste Lösung für die Messung von Teilentladung (TE), die speziell für den Einsatz in der Elektromobilität entwickelt und optimiert wurde. Mit PD-HVX kann TE bereits frühzeitig im Entwicklungsprozess gemessen und beseitigt werden.

Drei Fragen zu elektrischer Teilentladung an den Experten

Dr. Michael Stapelbroek, Vice President Electric Powertrain bei FEV

In der elektrischen Anlagentechnik ist das Phänomen Teilentladung (oder Partial Discharge) bereits seit langem bekannt. Wieso kommt es erst jetzt allmählich in der Automobilindustrie auf die Agenda?

Durch die zunehmende Verbreitung von 800 V DC-Systemen im Bereich der elektrischen Antriebe ist das Risiko für das Auftreten von TE um ein Mehrfaches gestiegen. Wie in allen elektrischen Systemen kann TE in der EDU zu Schäden an der Isolation und langfristig zum Ausfall des Fahrzeugs führen.

Welche Leistungen bietet FEV seinen Kunden im Kontext von TE ganz konkret an?

PD-HVX ist eine umfassende Systemlösung. Das kombinierte Hard- und Softwarepaket wurde speziell für den Einsatz in der Elektromobilität optimiert. Zum Gesamtpaket gehören die Schulung, die Inbetriebnahme der Messtechnik beim Kunden, eine detaillierte Analyse der Messdaten und daraus abgeleitete Maßnahmen. Mit mehr als 25 Jahren Erfahrung im Bereich der Messung und Beseitigung von TE beraten wir unsere Kunden bei ihrer Beseitigung bereits während des Entwicklungsprozesses.

»Das Ziel für den Kunden: Eine vollständig flexible und modulare batterieelektrische Plattform für leichte Nutzfahrzeuge.«

#7
Iveco New Daily Electric ***Serienentwicklung:*** Eine erfolgreiche Partnerschaft zwischen FEV und der Iveco Group

Iveco ist seit Jahrzehnten als führender Hersteller von Nutzfahrzeugen in allen Klassen und Segmenten bekannt. Charakteristisch für Iveco ist eine hochgradig anpassbare Fahrzeugplattform mit zahlreichen Varianten einschließlich spezieller Schnittstellen für den Markt der Aufbauhersteller („Body-Builder"). Dieses Alleinstellungsmerkmal muss auch bei der Umstellung auf batterieelektrische Fahrzeuge beibehalten werden, so dass Iveco eine hochflexible, modulare und kostengünstige Plattform für leichte Nutzfahrzeuge anstrebt.

Maßgeschneidertes Systems-Engineering, intelligente Architekturen und Kräftebündelung

Iveco hat mit dem Kernteam der ehemaligen Altra s.p.a. in Genua bereits seit 2009 erste Erfahrungen mit dem elektrischen Daily in sehr kleinen Stückzahlen sammeln können. Um diese Erfahrungen auszubauen und die Elektrifizierung in die regulären Serienentwicklungszyklen zu integrieren, bat Iveco FEV bei Strategie- und Technikaspekten um Unterstützung. Durch die gemeinsame Arbeit entstand eine langfristige und stabile Partnerschaft, die stetig gewachsen ist und bis heute erfolgreich andauert. Im Folgenden werden die Schlüsselfaktoren für den Erfolg des Fahrzeugs und die Zusammenarbeit der beiden Unternehmen beschrieben.

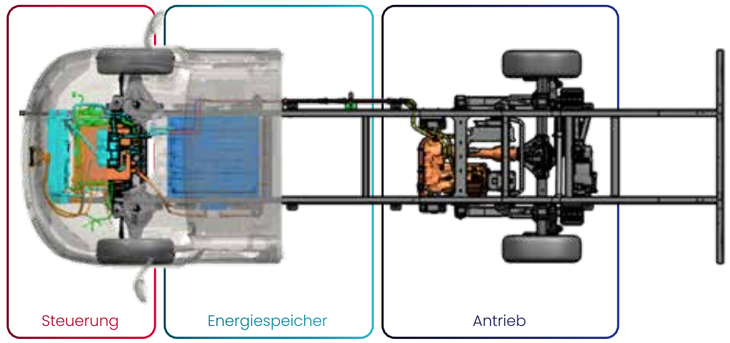
Zielorientierte und kontinuierliche Erarbeitung der Fahrzeugplattform

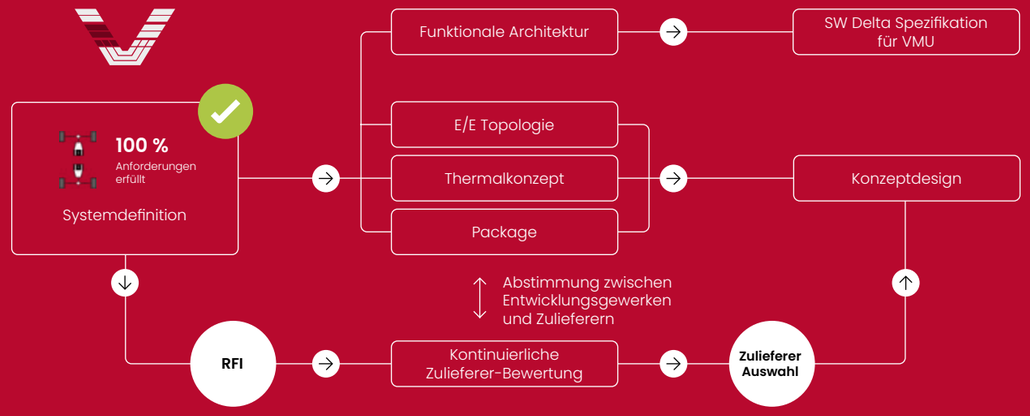
Die Zieldefinition einer kompletten Fahrzeugplattform erfordert in der Regel viel Zeit für die detaillierte Bewertung zahlreicher Varianten. Um diesen Prozess zu beschleunigen, begleitete FEV Consulting die ersten Phasen der Machbarkeitsbewertung und Konzeptdefinition der geplanten Umrüstung von Dieselantrieb auf batterieelektrischen Antrieb (Battery Electric Vehicle, BEV). Hierfür wurden sowohl Schlüsselvarianten als auch ausgewählte Ziele für jede Entwicklungsphase definiert und bewertet. Mit diesem Ansatz konnte die Gesamtplattform stetig und zielgerichtet weiterentwickelt werden und diente den Engineeringteams von FEV und Iveco als Grundlage für die erste Konzept- und Komponentenauslegung.

FEVs systematischer und simulationsbasierter Ansatz ermöglichte es, sehr früh mit internen und externen Abstimmungen zu beginnen, während gleichzeitig eine umfassende Plattformbewertung von mehr als 150 Varianten und variantenspezifischen Anwendungsfällen Schritt für Schritt hinzugefügt wurde. Auch mit der detaillierten Konzeptentwicklung konnte frühzeitig begonnen werden, was zu einem vollständig modularen Ansatz in Bezug auf Systemauslegung, E/E-Architektur und Thermal-Layout führte. Der Prozess wurde während der gesamten Konzeptphase durch Quervergleiche mit der wachsenden Anzahl an Varianten stetig überprüft. Dies führte bereits nach fünf Monaten zu einer robusten Zielsetzung und einem geeigneten Konzeptdesign.

1.
Zu elektrifizierende Varianten des Iveco Daily (Cab, Van, Crew Cab (4,25 t–7,2 t zGG)), Chassis Cowl und Minibus (7.2 t zGG)).

2.
Designbereiche der modularen Systemarchitektur des Iveco New Daily Electric.





3.
Konzeptphase mit parallelen Entwicklungspfaden und Lieferantenbewertung.

Komponentenorientierte Architekturentwicklung und schnelles Konzeptdesign
Wenn nicht nur eine Fahrzeugvariante, sondern eine komplette Plattform eingeführt wird, ist die Robustheit aller Fahrzeugteile zwingend erforderlich. Daher wird die Verwendung vorhandener, vorab geprüfter Standardkomponenten bevorzugt (Off-the-shelf-Komponenten). Eine Ausnahme bildet die Hochvoltbatterie, auf die später eingegangen wird.

Ein Abgleich zwischen System-Auslegung, der E/E-Architektur und den technischen Anforderungen aller Komponenten wurde kontinuierlich vorgenommen. Zusätzlich hat ein fortlaufender Austausch mit unterschiedlichen Lieferanten stattgefunden. Das Ergebnis ist heute ein sehr modulares Design, das klar definierte Bereiche für Energiespeicher, Antrieb und Steuerung des Fahrzeugs vorweist (Abb. 2, S. 41).

Parallel zur Lieferanten- und Komponentenbewertung wurden die Systementwicklung und das vollständige Konzeptdesign im Detail durchgeführt (Abb. 3). Hierbei kam das „Beste aus beiden Welten" zum Tragen – einerseits die Hochvolt(HV)-Erfahrung des Iveco Teams in Genua sowie das spezifische Wissen des Unternehmens über die eigenen Nutzfahrzeugplattformen. Andererseits die langjährige Erfahrung von FEV in der Elektrifizierung und Serienentwicklung von hybrid- und batterieelektrischen Fahrzeugen sowie Hochvoltbatterien.

Werkzeuggestütztes Anforderungsmanagement und frühe Validierungsplanung
Startpunkt für das Anforderungsmanagement waren die neuen Vorgaben der Stakeholder, die mit den IVG-Standardformaten für Lastenhefte zusammengeführt wurden. Das beinhaltete sowohl neue Hochvolt-Komponenten als auch die Standardfahrzeugfunktionen für alle systemweiten funktionalen Anforderungen, sowohl für neue als auch bestehende Funktionalitäten. Ivecos Standard-Fahrzeug-Validierungsplan wurde mit Hilfe der Elektrifizierungs-Expertise von FEV erweitert und mit den detaillierten Anforderungen an neuen HV-Komponenten verknüpft.

eVECOp, die modulare Inhouse-E-Antriebs-Plattform
Um den Off-the-shelf-approach auch für die Steuergerätesoftware zu wahren, wurde eine intelligente Funktionale Architektur definiert. Sie legt ein Soft-Gateway und andere notwendige Anpassungen für sämtliche Komponentenfunktionen innerhalb des hauseigenen E-Antriebs-Steuergeräts „VMU (Vehicle Management Unit) fest. Mit „eVECOp" wurde die Iveco interne Software des ersten Daily Electric zu einer vollständigen E-Antriebs-Steuerung ausgebaut. Alternativ bietet aber auch FEV seinen Kunden für derartige Anwendungsfälle eine eigens entwickelte Antriebs-Steuerungsplattform an.

Modulares FPT-Batteriesystem mit Master-BMS und Kunden-Feldversuch mit FEV Batterie
Das Batteriesystem besteht aus mehreren identischen Batterien, die im Leiterrahmen des New Daily Electric untergebracht sind und von einem Master-Battery Management System (BMS) koordiniert werden. Die heute eingesetzten Batterien werden hausintern von FPT-Industrial hergestellt, das Teil der Iveco Gruppe ist und auf einem Joint Venture mit Microvast basiert. Da jedoch die Batterieproduktion und die entsprechende Entwicklung parallel zum Fahrzeugprojekt aufgebaut werden mussten, wurde in der ersten Phase des Programms eine Zwischenlösung genutzt. Basierend auf Zellmodulen und Teilkomponenten eines bestehenden Pkws entwickelte FEV ein Prototyp-Batteriepack mit neuem Package sowie neuer Kühlung (Abb. 4). Die Batterien wurden in der FEV Proto-Werkstatt gebaut und die vollständige ECE R100-Konformitätsprüfung in FEVs eDLP, dem weltweit größten unabhängigen Entwicklungs- und Testzentrum für Hochvoltbatterien, durchgeführt. Das Master-BMS für die ersten Fahrzeuge nutzte die FEV eigenen „Multi-Batterie-String-Funktionen", um die bis zu drei Batterie-Packs untereinander zu koordinieren und aus Sicht des restlichen Antriebs als einen Gesamt-Energiespeicher darzustellen.

Um so früh wie möglich praxisrelevante Felddaten sammeln zu können, stellte Iveco einem Endkunden zwei reife Alpha-Prototypenfahrzeuge zur Verfügung. Die meisten HV-Komponenten waren bereits in der Zielvariante enthalten. Dazu zählten neben den Prototyp-Batterien von FEV die „eVECOp"-Steuerungen, und FEVs Master-BMS, die beide auf einer dSpace MicroAutobox® als Rapid-Control-Plattform laufen. Diese Fahrzeuge wurden auf Basis von Einzeltypgenehmigungen für den europäischen Markt zugelassen (Prototypenfreigabe für geschulte Fahrer) und waren auf Seiten des Endkunden mehrere Monate lang vollständig in den regulären Geschäftsbetrieb eingebunden. Ein gemeinsames „Flying-Doctor"-Team von FEV und der Iveco Gruppe wurde zusammengestellt und blieb für die kontinuierliche Wartung, Datenerfassung und -analyse in engem Kontakt mit dem Kunden. Auf diese Weise konnten nicht nur wertvolle Einblicke in die reale Anwendung gewonnen werden, sondern auch ein qualitativ hochwertiger Konzeptnachweis im Feld erbracht werden. Diese ersten Prototypenfahrzeuge sind auch heute noch zuverlässig im Einsatz.

Ganzheitlicher Projektansatz
Ein weiterer Erfolgsfaktor war das Projekt-Setup selbst. Es umfasste nicht nur die technische Entwicklung, sondern auch die frühzeitige Fertigungsplanung und die Schulung der erweiterten Iveco Teams im Bereich der Elektrifizierung. Eine kontinuierliche parallel erfol-

4.
Von FEV entwickeltes Batteriepaket für den frühen Feldtest des New Daily Electric.

gende strategische Unterstützung durch FEV Consulting sicherte darüber hinaus den Überblick in dem bis dato noch volatilen Marktumfeld.

Die Zusammenstellung und Zusammenarbeit von unterschiedlichen Teams in großen Projekten ist immer eine Herausforderung, die im Rahmen dieser Kooperation erfolgreich implementiert wurden. So wirkten sowohl seitens FEV als auch Iveco mehrere Standorte an dem Projekt mit: in Italien zählten für Iveco neben dem Unternehmenshauptsitz in Turin das Produktionswerk in Suzzara und das Kompetenzzentrum für Elektrifizierung in Genua dazu. Auf Seiten von FEV trugen Experten vom Hauptsitz in Aachen, von FEV Italia in Turin und weiteren Standorten der Tochtergesellschaften FEV France und FEV Türkiye erfolgreich zum Projekterfolg bei.

Gemeinsamer Erfolg: Der Iveco New Daily Electric

Seit April 2023 ist der New Daily Electric offiziell erhältlich. Der frühe Programmstart mit dem klaren Ziel, ein breites Spektrum an batterieelektrischen Anwendungsfällen zu adressieren, hat sich ausgezahlt – die Leistung und die Flexibilität des Produkts haben höchste Erwartungen erfüllt.

Alle Standard-Aufbauvarianten von Iveco werden abgedeckt, ebenso wie der gesamte Daily Gewichtsbereich von 3,5 bis 7,2 t GVW (Gross Vehicle Weight, zulässiges Gesamtgewicht). Ebenso werden alle Radstände von 3.000 mm bis 4.750 mm als vollelektrische Versionen angeboten, wobei das übliche Iveco Versprechen für hohe Nutzlast und Ladevolumen aufrechterhalten wird.

Die Batterien des modularen Batteriekonzepts werden innerhalb der Iveco Gruppe hergestellt, Konfigurationen mit einer WLTP-Reichweite von bis zu 300 km und einer unter realen städtischen Bedingungen getesteten Reichweite von 400 km werden angeboten. Das Aufladen ist mit bis zu 22 kW bei Wechselstromaufladung und 80 kW bei Gleichstromaufladung möglich, was einer Reichweitenwiederherstellung von bis zu 100 km in nur 30 Minuten entspricht.

Die HV-Architektur und ihre Integration in die modularen Designzonen (Abb. 2, S. 41) ermöglicht nicht nur die Wahl der Batteriekonfiguration, sondern bietet auch höchste Flexibilität für die Aufbauhersteller. Das flache und robuste Grundchassis ermöglicht Umbauten und bietet drei verschiedene Arten von elektrischen und mechanischen Nebenantrieben (Power Take-Off), die den Aufbauherstellern einen noch größeren Freiheitsgrad als bei den Dieselversionen bieten.

Schließlich sorgt der 140 kW/400 Nm starke Elektromotor in Kombination mit zwei oder drei Batterien für ideale Fahrleistungen sowie eine Steigfähigkeit von bis zu 30 Prozent und 3,5 t Anhängelast. Die Iveco typische Robustheit wurde von -30 °C bis zu +50 °C getestet.

WLTP-Reichweiten

zGG	1 Batterie	2 Batterien	3 Batterien
3,5 t	120 km	235 km	
4,25 t	110 km	200 km	300 km
5,2 t		185 km	260 km
7,2 t		120 km	180 km

5.
Fahrzeugvarianten mit zulässigem Gesamtgewicht (zGG) und Batteriekonfigurationen sowie WLTP-Reichweiten.

6.
Zusammenarbeit von Iveco Group, Iveco Electrification Competence Center, FEV Engineering und FEV Consulting.

Ausblick

Das vorgestellte ehrgeizige und erfolgreich abgeschlossene Projekt hat eine stabile, vertrauensvolle und langfristige Partnerschaft zwischen der Iveco Group, FEV Consulting, dem Iveco Electrification Competence Center und den Engineering-Bereichen bei FEV etabliert. Als Schlüsselfaktoren für den Erfolg erwiesen sich die flexible Architektur, modernste Entwicklungsprozesse und -werkzeuge sowie die dynamische und globale Projektstruktur – aber auch der gemeinsame Antrieb, für jede Herausforderung eine Lösung zu finden.

An der weiteren Zukunft des Iveco New Daily Electric wird heute bereits gearbeitet: Inzwischen wurde eine Brennstoffzellenversion entwickelt und entsprechende Prototypen-Fahrzeuge aufgebaut sowie der Öffentlichkeit vorgestellt. Das Update des New Daily Electric für das Modelljahr 2024 wurde ebenso angekündigt und feiert in Kürze seine Markteinführung. Das modulare Konzept wird hierbei konsequent beibehalten und weiter optimiert, u. a. durch eine spezielle Variante mit einem vierten Batteriepaket und verbessertem Schnellladen.

VON
Dr. Felix Richert, FEV
richert@fev.com
Patrick Glusk, FEV
glusk@fev.com
Alessandro Bernardini, Iveco Group
Marco Aimo-Boot, Iveco Group

#8

Proprietäre Lösungen

Feel EVolution bei FEV

FEVs proprietäre Lösungen ermöglichen es dem Unternehmen, sich am Markt mit einzigartigen Entwicklungen abzuheben und seinen Kunden den entscheidenden Wettbewerbsvorteil zu verschaffen. Wir stellen im SPECTRUM regelmäßig eine Auswahl dieser Lösungen vor.

Weitere Informationen zu FEVs proprietären Lösungen

Vehicle Motion Control (VMC) – Software zur Drehmomentverteilung bei Fahrzeugen mit elektrischem Antriebsstrang

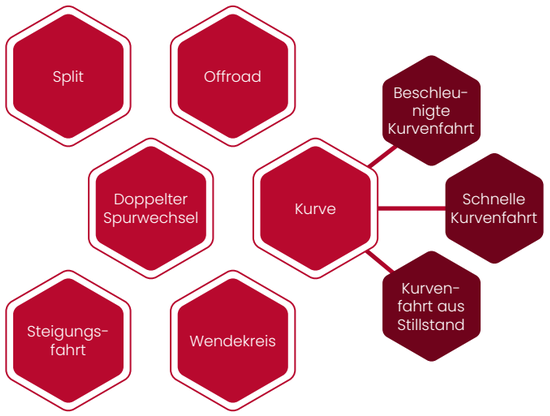
Die Vielfalt elektrifizierter Fahrzeuge umfasst unterschiedliche Antriebsarchitekturen, die sich vor allem in Anzahl, Position und Typen der Maschinen unterscheiden. Darüber hinaus wird die Antriebsstrangsteuerung zunehmend in ein domänenübergreifendes System, die Vehicle Motion Control (VMC), integriert. Bei dieser wird die Drehmomentverteilung in eine gesamtheitliche Bewegungssteuerung des Fahrzeuges integriert, um die Fahrzeugdynamik durch eine koordinierte Ansteuerung von Bremse und Antrieb zu kontrollieren.

Um diesen Anforderungen gerecht zu werden, hat FEV die eigene Software-Bibliothek kontinuierlich weiterentwickelt. Dabei ermöglicht die Modularität der Software eine einfache Anpassung an verschiedenste Antriebsarchitekturen sowie eine gleichzeitige Umsetzung von fahrdynamischen Vorgaben.

Um eine höhere Reichweite zu erzielen, muss das Antriebssystem so gesteuert werden, dass die elektrische Energie möglichst effizient genutzt wird, um Verluste zu minimieren. Dazu werden Effizienzmodelle aller beteiligten Antriebsstrangkomponenten in die Verteilungsstrategie der Drehmomentsoftware integriert. Besonders wichtig ist dies bei Architekturen mit verschiedenen Arten von Maschinen, wo die Auswahl spezifischer Betriebspunkte relevant ist. Die Reduzierung von Verlusten erfolgt durch eine integrierte Optimierung, die vorhandene Leistungs- und Drehmomentbeschränkungen berücksichtigt.

Darüber hinaus ermöglicht die FEV Software ein verbessertes Fahrverhalten sowie situativ erhöhte Traktion, indem übertragbare Radkräfte geschätzt und der Radschlupf überwacht werden. Bei drohendem Traktionsverlust erfolgt eine Umverteilung der Drehmomente auf die verbleibenden angetriebenen Räder. Diese Funktionalitäten sind besonders für Off-Road-Fahrzeuge und mobile Antriebsmaschinen notwendig, da sowohl die Eigenschaften des Untergrunds stark variieren als auch ein Kontaktverlust mit dem Untergrund auftreten kann.

Bei Topologien mit mehreren Maschinen je Achse ist eine Verbesserung des lateralen Fahrzeugverhaltens möglich. Aus der Sollvorgabe der Fahrzeugbewegungen wird ein Drehmomenteingriff abgeleitet, welcher die Gierrate beeinflusst und den Schwimmwinkel begrenzt. Dadurch wird sowohl ein verbessertes Kurvenverhalten als auch eine erhöhte Manövrierbarkeit bei Ausweichmanövern erzielt. Bei Abweichungen des Verhaltens vom Sollzustand (z. B. µ-Split) greift die Vorsteuerung des Antriebsstrangs in die Fahrzeugdynamik ein. Diese Vorsteuerung wirkt sich stabilisierend auf das Fahrzeug aus und reduziert Eingriffe des ESP.



VON
Dr. Rene Savelsberg,
savelsberg@fev.com
Björn Krautwig,
krautwig@mmp.rwth-aachen.de

Modular Fuel Cell Control Software

Um die strengen CO_2-Regeln zu erfüllen, ist die Nutzung von Wasserstoff als Energieträger für die Mobilität vielversprechend. Die Entwicklung von Proton Exchange Membrane (PEM)-Brennstoffzellen sticht hierbei hervor, da sie sowohl für die Straße und für das Gelände geeignet sind, sie keine CO_2-Emissionen verursachen, eine hohe Energiedichte aufweisen und schnell anlaufen. Ihre Leistungsfähigkeit hängt jedoch eng mit den eingesetzten Steuerungskonzepten zusammen, um das Ziel zu erreichen, einen hohen Wirkungsgrad, ein reibungsloses Einschwingverhalten, langfristige Zuverlässigkeit, Langlebigkeit und allgemeine Sicherheit während des Betriebs zu gewährleisten.

Um diesen Herausforderungen zu begegnen, hat FEV eine modulare Fuel Cell Control Unit (FCCU) Software entwickelt, die für verschiedene P&ID-Konfigurationen (Piping & Instrumentation Diagram) von Brennstoffzellensystemen verwendet werden kann. Die Software steuert und überwacht den Stack und die Balance of Plant (BoP)-Komponenten, stellt eine optimale Steuerungskoordination zwischen den verschiedenen Brennstoffzellen-Subsystemen her und kommuniziert mit dem Hauptfahrzeugsteuergerät. Die Steuerungssoftware verfügt über eine umfassende State-Machine, die das Ein- und Ausschalten des Systems einschließlich der Einfriervermeidung steuert, was mit verschiedenen Brennstoffzellenherstellern abgestimmt wurde. Wesentliche leistungsbeeinflussende Steuerungsparameter wie Temperatur, Druck, Feuchtigkeit und Luftstöchiometrie werden sorgfältig ermittelt und geregelt. Je nach Systemkomplexität setzt die modulare Software verschiedene Strategien zur Massenstrom-, Druck- und Feuchteregelung ein, z. B. mit Drosseln und Bypässen. Besonderes Augenmerk wird auf die Optimierung der Purge/Drain-Strategie gelegt. Durch eine Leistungsregelung im geschlossenen Regelkreis mit Fokus auf die Degradationsmodellierung zur Lebensdauerverlängerung der Brennstoffzelle können Komponentenunterschiede oder die Alterung berücksichtigt werden. Zudem können durch Überwachungs- und Diagnosefunktionen frühzeitig Fehler erkannt werden, wodurch Stack-Schäden minimiert und ein sicherer Betrieb gewährleistet werden.

Die Steuerungssoftware wurde erfolgreich in verschiedene Prototyp- und Seriensteuergeräte integriert und hat ihre Fähigkeiten durch Tests an Brennstoffzellenprüfständen und Fahrzeugen unter Beweis gestellt. Die Software kann in die FEV Steuerungslösungen für VCU/HCU (Vehicle/Hybrid Control Unit) zur übergeordneten Steuerung integriert oder mit der Software des Kunden gepaart werden. Zusätzlich ermöglicht die White-Box-Option Kunden, FEVs Lösung für ihre eigene Steuerungsentwicklung zu nutzen.

VON
Dr.-Ing. Vivek Srivastava,
srivastava_vivek@fev.com
Dr.-Ing. Joschka Schaub,
schaub@fev.com
Dr.-Ing. Marius Walters,
walters_m@fev.com

mehr als

7.500 FEV Experten weltweit

FEV Europe GmbH
Neuenhofstraße 181
52078 Aachen
Deutschland
T +49 241 5689-0
marketing@fev.com

FEV North America, Inc.
4554 Glenmeade Lane
Auburn Hills
MI 48326-1766 · USA
T +1 248 373-6000
marketing@fev-et.com

FEV China Co., Ltd.
168 Huada Road
Yanjiao High-Tech Zone
065201 Sanhe City
Langfang Hebei Province
China
T +86 10 80 84 11 68
fev-china@fev.com

FEV India Pvt, Ltd.
Technical Center India
A-21, Talegaon MIDC
Tal Maval District
Pune 410 507 · Indien
T +91 2114 666-000
fev-india@fev.com

RECYCLED
Papier aus Recyclingmaterial
FSC® C106855

SPECTRUM #78
Ausgabe 01/2024

Redaktion
Marius Strasdat
FEV Europe GmbH

Gestaltung
Verena Mainz
FEV Europe GmbH

Leserservice
Sie möchten regelmäßig SPECTRUM erhalten oder Ihre Anschrift hat sich geändert? Senden Sie Namen, Unternehmen und Anschrift per E-Mail an
spectrum@fev.com

company/fev-europe

feel evolution

fev.com