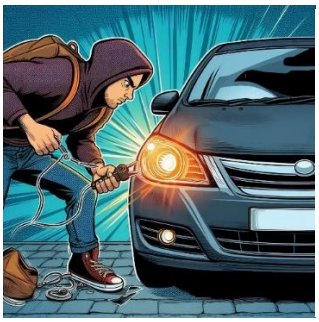
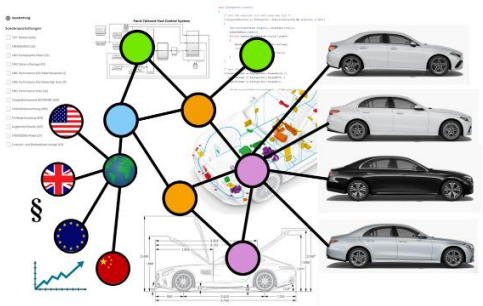
# Verbesserung von Cybersecurity Untersuchungen und davon abgeleiteten Massnahmen mit Hilfe von TPLE

Ein Beitrag im Förderprojekt Software-Defined Car


Quellen links und rechts: Microsoft Bing Image Creator, in der Mitte: Mercedes-Benz AG


## Kurzfassung

Die rasante Entwicklung der Digitalisierung, Konnektivität und Automatisierung in Fahrzeugen hat die Möglichkeiten des Missbrauchs durch Kriminelle erweitert, die von der Manipulation sicherheitskritischer Funktionen bis hin zum unberechtigten Datenzugriff reichen. Als Reaktion darauf hat die UNECE die R155-Verordnung erlassen, welche die Hersteller (OEMs) dazu verpflichtet, robuste Sicherheitsmaßnahmen zu implementieren. Die enorme Vielfalt der Fahrzeuge, gepaart mit zahlreichen elektrischen Komponenten, die von verschiedenen Anbietern bezogen werden, und einem softwaregesteuerten Entwicklungsansatz führt jedoch zu einem exponentiellen Anstieg der Varianten. Diese Komplexität, die oft mit Hilfe unterschiedlicher Datenquellen verwaltet wird, stellt die OEMs vor große Herausforderungen, wenn es darum geht, umfassende und schnelle Reaktionen auf Cybersicherheitsvorfälle für alle potenziell betroffenen Fahrzeuge zu gewährleisten. In diesem Beitrag wird untersucht, wie Typebased Product Line Engineering (TPLE) diesen Prozess beschleunigen kann, um die Cybersicherheit ihrer Fahrzeuge zu verstärken.



Autoren

Thomas Bitterlich, T-Systems International GmbH
Grit Pientka, T-Systems International GmbH
Chris Seiler, Mercedes-Benz AG

# EINFÜHRUNG

## INSPIRIERT VON EINEM REALEN CYBERSECURITY ANGRIFF

Am 3. April 2023 enthüllte Ken Tindell in einem Blogbeitrag [1] einen schlüssellosen Autodiebstahl. Der Diebstahl wurde über ein externes, im Darknet verfügbares Gerät ausgeführt, das mit einem fahrzeuginternen CAN-Bus verbunden wurde. Die folgenden Ausführungen basieren auf einer Zusammenfassung des Diebstahls, wie sie von Tindell beschrieben wurde.

## DER ANGRIFF IN KÜRZE

Der schlüssellose Diebstahl erfolgt durch die physische Verbindung eines CAN-Injektionsgeräts, das im Darknet für mehrere tausend Euro erhältlich ist, mit dem Chassis-Bus in einem geparkten Fahrzeug. Diese Geräte gibt es in einer Vielzahl von Varianten, die jeweils für ein bestimmtes Fahrzeugmodell zahlreicher OEMs entwickelt wurden.

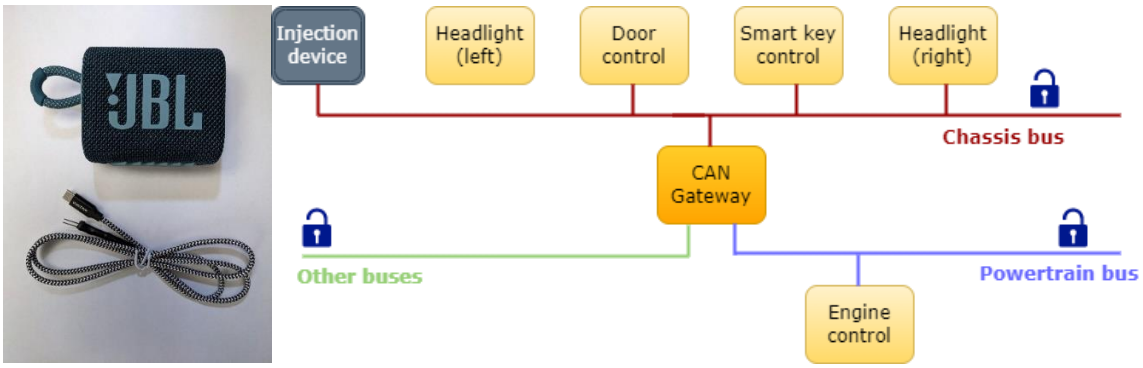



**ABBILDUNG 1: LINKS - ABBILDUNG DES IN EINEN BLUETOOTH-LAUTSPRECHER EINGEBAUTEN CAN-BUS MANIPULATIONSGERÄTS (INJECTION DEVICE) AUS [1]. RECHTS - GROBER ÜBERBLICK ÜBER DAS E/E-NETZWERK DES BETROFFENEN FAHRZEUGS**

Eine Verbindungsmöglichkeit besteht darin, den CAN-Bus Stecker eines Scheinwerfer-Steuergeräts (im vorliegenden Fall das linke, wie in Abb. 2 dargestellt) zu verwenden, das durch Entfernen der seitlichen Stoßstange des Fahrzeugs zugänglich ist, vgl. Abb. 2. Sobald das Gerät angeschlossen ist, unterbricht es die reguläre Kommunikation auf dem Chassis-Bus und sendet hochfrequente Befehle, um die Wegfahrsperre zu deaktivieren, den Motor zu starten und die Türen zu öffnen. Die Befehle zum Motorstart müssen ein CAN-Gateway passieren, um das Motorsteuergerät zu erreichen (vgl. Abb. 1). Aufgrund der gestörten Busarbitrierung setzt das CAN-Gateway den CAN-Transceiver permanent

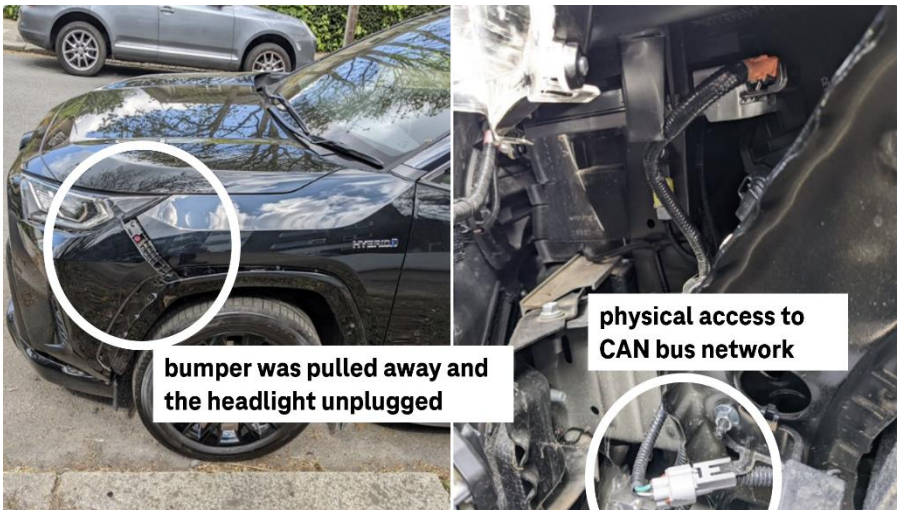



**ABBILDUNG 2: DARSTELLUNG, WIE DER PHYSISCHE ZUGRIFF EINES BETROFFENEN FAHRZEUGS REALISIERT WERDEN KANN [1]**

zurück und leitet die Nachricht während eines der anschließenden Neustarts an den Powertrain-Bus weiter.

Dieses Szenario ist eine Katastrophe für den Fahrzeugbesitzer, die Versicherungsgesellschaften, die den Schaden decken, sowie für die Hersteller, deren Ruf durch die Leichtigkeit des Fahrzeugdiebstahls geschädigt wird. Infolgedessen haben bereits viele Versicherungsgesellschaften entweder die Diebstahldeckung für die am häufigsten gestohlenen Modelle verweigert, zusätzliche Diebstahlschutzmaßnahmen gefordert oder die Prämien erhöht [2].

## Gesetzgeberische Anforderungen

Die ISO21434 [3] und die UNECE R155 [4] verpflichten die OEMs, die Cybersicherheit ihrer Fahrzeugflotte kontinuierlich zu überwachen und potenzielle Cybersicherheitsprobleme zu erkennen und zügig zu behandeln. Diese komplexe Aufgabe erfordert die Einbindung eines Systems zur Überwachung der Fahrzeugsicherheit in ein von der UNECE R155 vorgeschriebenes Cyber Security Management System (CSMS). Doch die Erkennung von Cybersicherheitsvorfällen allein reicht nicht aus. Nach der Bestätigung von Schwachstellen müssen Verfahren zur Schadensbegrenzung eingeleitet und für alle potenziell betroffenen Fahrzeuge umgesetzt werden. Der Prozess der Schadensbegrenzung bei Cyber Security-Vorfällen umfasst die folgenden Phasen:

1. Analyse, um die Ursache der Bedrohung zu ermitteln und alle betroffenen Fahrzeuge zu identifizieren.
2. Soforthilfemaßnahmen, soweit möglich.
3. Entwicklung eines Sicherheitspathes unter Berücksichtigung aller Software- und Hardwareanforderungen (kurzfristig).
4. Ausrollen des Sicherheitspatches, entweder per Over-the-Air Update oder in Werkstätten. Dies kann eine vorangehende erfolgreiche Homologation erfordern, bevor der Patch verteilt werden kann.
5. Identifizierung und Umsetzung langfristiger Maßnahmen zur Verhinderung von Varianten des entdeckten Angriffs und zur Verbesserung der Sicherheit künftiger Fahrzeuggenerationen.

In jeder dieser Phasen muss die große Anzahl von Fahrzeugvarianten berücksichtigt werden.

## Fragen, die sich bei der Untersuchung des schlüssellosen Fahrzeugdiebstahls stellen

### Phase 1: Analyse

- ***Was sind die gemeinsamen Features der betroffenen Fahrzeuge?***
  Im Falle des CAN-Injektions-Angriffs ist dies
  - Die E/E-Architektur: sowohl das Scheinwerfer Steuergerät als auch das Smart Key Steuergerät befinden sich auf dem Chassis-Bus.
  - Der Chassis-Bus ist von außen zugänglich.
  - Das Smart Key Steuergerät überträgt Nachrichten ohne Authentifizierung.
- ***Welche anderen Fahrzeuge weisen die gleichen oder ähnliche Features auf und sind damit ebenfalls anfällig für diesen Angriff?***
  Dies gilt für alle Fahrzeugtypen, bei denen
  - Das Smart Key Steuergerät Nachrichten ohne Authentifizierung versendet.
  - Sich das Scheinwerfer Steuergerät und das Smart Key Steuergerät auf einem Bus befinden,
    und/oder
  - Sich das Smart Key Steuergerät auf einem Bus befindet, der möglicherweise von außen zugänglich ist.

### Phase 2: Unmittelbare Abhilfemaßnahmen

- ***Wie können die gefährdeten Fahrzeuge schnell davor geschützt werden, Opfer des Angriffs zu werden?***
  Eine Option könnte die Implementierung eines Sicherheits-Patches sein. Im vorliegenden Fall beispielsweise durch Einführung von signierten Nachrichten vom Smart Key Steuergerät.
- ***Gibt es Maßnahmen, die auf Fahrzeuge angewendet werden können, die bereits erfolgreich angegriffen und gestohlen wurden? Ist es zum Beispiel möglich, das Fahrzeug sicher außer Betrieb zu nehmen?***
  Diese Beantwortung der Frage ist insbesondere interessant, um zukünftig Diebstähle zu verhindern oder bereits entwendete Fahrzeuge zu lokalisieren. Die Fahrzeuginsassensicherheit muss bei eingeleiteten Maßnahmen jederzeit gewährleistet bleiben.

### Phase 3: Entwicklung eines Sicherheitsupdates

- ***Welche Software- und Hardware-Abhängigkeiten bestehen für die verschiedenen bedrohten Fahrzeugtypen, die bei der Entwicklung eines Sicherheitspatches berücksichtigt werden müssen?***
  Im beschriebenen Beispiel stellt sich die Frage, ob beispielsweise sichere Onboard Kommunikation (secOC) für die Nachrichten des Smart Key Steuergerätes eingeführt werden kann. Dies ist nur möglich, wenn alle an der Kommunikation beteiligten Steuergeräte dazu in der Lage sind.

### Phase 4: Ausrollen des Sicherheitspatches

- ***Wie kann das Sicherheitspatch an alle gefährdeten Fahrzeuge verteilt werden?***
  Dies kann Over-the-Air-Updates, Rückrufe von Fahrzeugen oder die Aktualisierung von Fahrzeugen während des regulären Werkstattaufenthalts beim Kundendienst umfassen. Das tatsächliche Vorgehen hängt von den verfügbaren Funktionen der Fahrzeuge, der Schwere der Sicherheitslücke und möglicherweise von den Entscheidungen der Typgenehmigungsbehörden ab, die über jeden festgestellten Angriff informiert werden müssen.
- ***Sind die durch den Patch eingeführten Änderungen für die Typgenehmigung relevant?***
  Das Smart Key Steuergerät kann durchaus typgenehmigungsrelevant sein, so dass ein Homologationsverfahren für den Sicherheitspatch erforderlich wird.
- ***Welche spezifischen Fahrzeuge (VINs) sollen welchen Patch erhalten?***
  Dies hängt von der Software- und Hardware-Konfiguration jedes einzelnen Fahrzeugs ab. Unter Umständen ist es erforderlich, unterschiedliche Patches für unterschiedliche Konfigurationen zu erstellen und auszurollen.

### Phase 5: Langfristige Maßnahmen

- ***Welche Verallgemeinerungen oder Varianten des Angriffs könnten in Zukunft auftreten, und welche Auswirkungen hätten diese auf die Fahrzeuge?***
  Beispielsweise könnten die Angreifer andere Möglichkeiten ausnutzen, um ein externes Gerät physisch mit einem CAN-Bus zu verbinden, der das Smart Key Steuergerät enthält.
- ***Welche langfristigen Maßnahmen können ergriffen werden, um zukünftige Angriffe zu verhindern, und sind diese für die Typgenehmigung relevant?***
  Ken Tindell schlägt die Verwendung von Hardware-Sicherheitsmodulen vor, um bestimmte CAN Nachrichten zu verschlüsseln. Weitere Optionen wären die Einführung von sicherer Onboard-Kommunikation (Secure Onboard Communication - SecOC) im Allgemeinen oder zumindest (teilweise) auf dem Chassis Bus oder die Änderung der Position des Smart Key Steuergeräts in der E/E Architektur des Fahrzeugs.

Diese Fragen erfordern Sicherheits- und technisches Fachwissen, insbesondere in den Bereichen:

- Angriffserkennung[1]
- Analyse von Angriffsvektoren[2]
- Verstehen des Angriffs[3]
- Erkennung und Durchführung notwendiger Änderungen in der Bedrohungsanalyse und Risikobewertung (TARA)[4]

Aktuelle Variantenmanagementsysteme beschränken diese Untersuchungen auf die Varianten von jeweils einem Modell, einem Fahrzeugtyp oder auf eine Variante. Die Zusammenführung der Ergebnisse für alle betroffenen Modelle und Fahrzeugtypen ist mit manuellem Aufwand verbunden. Es ist dann eine Herausforderung sicherzustellen, dass alle betroffenen Fahrzeuge - wie in der Verordnung gefordert - erfasst wurden.

## Alle neu auftretenden Vorfälle im Bereich der Cyber Security erfordern sofortige Aufmerksamkeit

Täglich werden neue Sicherheitslücken, Schwachstellen, Bedrohungen, Exploits und Angriffe im Automobilsektor festgestellt, die jeweils sofortige Aufmerksamkeit und Reaktion erfordern. Die UNECE-Regelung R155 [4] verpflichtet die OEMs, dafür zu sorgen, dass ihre Fahrzeuge vor allen bekannten Bedrohungen geschützt bleiben, um die Fahrzeugnutzer zu schützen[5]. Die Nichteinhaltung kann zum Entzug der Typgenehmigung des Fahrzeugs führen.

---

[1] Die Erkennung eines Angriffs kann sehr komplex sein, was vor allem daran liegt, dass nur

- sehr wenige Fahrzeuge einer Fahrzeugflotte betroffen sind
- begrenzte Informationen zur Verfügung stehen
- die Auswirkungen, nicht aber die eigentliche Ursache sichtbar sind

Diese eingeschränkte Sichtweise kann es schwierig machen, die tatsächliche Quelle der Unregelmäßigkeiten zu ermitteln. So stellte sich beispielsweise in dem in dieser Abhandlung behandelten Fall heraus, dass das, was zunächst als Vandalismus Problem wahrgenommen wurde, tatsächlich ein versuchter Fahrzeugdiebstahl war, der durch ein externes Schadgerät ermöglicht wurde. Dies wurde erst entdeckt, nachdem das Auto gestohlen worden war und eine gründliche Untersuchung durchgeführt wurde (der Auslöser war auch ein kurz vorher gescheiterter Diebstahlsversuch, bei dem auch digitale Spuren hinterlassen wurden).
In anderen Szenarien können solche Angriffe nur durch umfassende, flottenweite Beobachtungen entdeckt werden. Dies unterstreicht die Notwendigkeit einer umfassenden Überwachung der ganzen Fahrzeugflotte, um potenzielle Bedrohungen der Cybersicherheit wirksam erkennen und bekämpfen zu können.

[2] Die Untersuchung des genutzten Angriffsvektors ist von größter Bedeutung. Dieses Verständnis bildet die Grundlage für die Ausarbeitung eines Plans zur Schadensbegrenzung und die Erstellung von Testfällen für die implementierten Sicherheitsmaßnahmen. Nur wenn der Angriffsweg gründlich analysiert wurde, können wirksame Gegenmaßnahmen entworfen und getestet werden.

[3] Ein umfassendes Verständnis des Angriffs ist erforderlich, um ihn in einer kontrollierten Umgebung zu replizieren. Diese Replikation ermöglicht eine präzise Simulation des Angriffs, die für die Prüfung und Validierung potenzieller Abhilfemaßnahmen erforderlich ist. Die Möglichkeit, den Angriff nachzustellen, stellt sicher, dass die implementierten Gegenmaßnahmen sicher sind und einen ähnlichen Angriff in der Zukunft erfolgreich verhindern können.

[4] Sobald der Angriff vollständig verstanden ist, muss die TARA unbedingt entsprechend angepasst werden. Dies könnte die Einbeziehung eines neu entdeckten Angriffsvektors oder die Anpassung des bewerteten Risikos auf der Grundlage der neu gewonnenen Erkenntnisse beinhalten. Im Fall des schlüssellosen Autodiebstahls könnte die Anpassung zum Beispiel eine Neubewertung der Eintrittswahrscheinlichkeit des Angriffswegs erfordern. Normalerweise wird der physische Zugriff auf ein Bussystem als sehr schwer durchführbar angesehen, was das Risiko insgesamt auf ein allgemein akzeptiertes Niveau reduziert. Die Entdeckung des schlüssellosen Autodiebstahls zeigt jedoch, dass diese Annahme überdacht werden muss. **Das kann sich in der TARA auch auf weitere Risikowerte auswirken**.

[5] Die Fahrzeuginsassen Sicherheit ist nur gegeben, wenn die Bedrohungen durch Cyber Security im Rahmen eines vertretbaren Restrisikos gehalten werden. Ansonsten ist ein Angreifer (zu) leicht dazu in der Lage, auch sicherheitskritische Funktionen im Auto zu steuern.

Im Falle von sicherheitskritischen Problemen, die seine Fahrzeuge betreffen, kann der Gesetzgeber den OEM dazu zwingen, die betroffenen Fahrzeuge zur Behebung zurückzurufen. Es liegt in der Verantwortung des OEM, alle betroffenen Fahrzeuge zu identifizieren und für alle eine Lösung des Problems zu finden und im Fahrzeug umzusetzen.

Die Fragen, die bereits im Zusammenhang mit dem schlüssellosen Fahrzeugdiebstahl gestellt wurden, lassen sich weitgehend verallgemeinern. Unter der Annahme, dass die betroffenen Fahrzeuge identifiziert wurden, lässt sich das Problem wie folgt zusammenfassen:

- Was sind die gemeinsamen Features der betroffenen Fahrzeuge?
- Welche Fahrzeugtypen oder -modelle könnten ebenfalls betroffen sein?
- Gibt es eine kurzfristige Lösung für alle betroffenen Fahrzeuge?
- Was ist die langfristige Lösung?
- Was sind die Schritte zur Umsetzung dieser Lösungen?
- Sind diese Lösungen homologationsrelevant?
- Wie sollen die Lösungen eingeführt werden?

Diese Fragen unterstreichen die komplexen Herausforderungen, denen sich OEMs im Zuge ständiger Cyber Security Bedrohungen gegenübersehen, und verdeutlichen die Notwendigkeit einer robusten und effektiven Reaktionsstrategie.

## Ziel: Rasche und zuverlässige Abhilfe

OEMs müssen Lösungen für auftretende Cyber Security Vorfälle in einem Tempo finden, das mit ihrer zunehmenden Häufigkeit Schritt halten kann. Wenn Bedrohungen der Insassensicherheit auftauchen, müssen diese Lösungen schnell verfügbar sein, da sofortige Abhilfemaßnahmen erforderlich sind und die unternommenen Anstrengungen der Zulassungsbehörde gemeldet werden müssen. Idealerweise sollte eine Echtzeitlösung zur Verfügung stehen, um diese Probleme zu lösen. Es muss unbedingt sichergestellt werden, dass alle direkt und potenziell betroffenen Fahrzeugvarianten in den Abhilfeprozess einbezogen werden.

## Methode

Die typische Lösung für zeitkritische Aufgaben mit hohem Volumen ist die Automatisierung. Mangels einheitlicher Datenbasis für die Komponenten und Features verschiedener Fahrzeugtypen ist dieser Prozess erschwert. Häufig sind diese Informationen über verschiedene Dateien / Datenbanken mit unterschiedlichen Formaten verstreut, so dass sie sich nicht automatisch analysieren lassen. Dies liegt an den historisch gewachsenen, hardware-zentrierten Entwicklungsprozessen, die auch heute noch in der Fahrzeugentwicklung weitgehend üblich sind.

## Der Status Quo: Wir stecken in der hardware-definierten Welt fest!

Gegenwärtig sehen wir in der deutschen Automobilindustrie Plattformentwicklungen auf der Ebene der elektronischen Steuergeräte und ihrer jeweiligen komponentenorientierten Peripherie (Sensorik, Aktorik), unterstützt durch den Einsatz von Off-The-Shelf PLM-Lösungen, welche die funktionsbasierte PLE-Methode (Product Line Engineering) [5] realisieren. Dies ermöglicht ein Produktportfolio auf Basis einer kundenindividuellen Massenproduktion, die die Herstellung von Fahrzeugen mit einem hohen Individualisierungsgrad ermöglicht.

Allerdings stößt dieser Ansatz an seine methodischen Grenzen:

- Es gibt keine klare Trennung von Anforderung und Realisierung.
- Der fachliche Kontext von Varianzpunkten wird nicht direkt dokumentiert.

- Die Semantik und der Kontext von Features werden nicht abgebildet.
- Es fehlen konkrete Aussagen über einzelne Produktinstanzen.
- Es ist kein umfassendes und konsistentes Änderungs- und Konfigurationsmanagement möglich.

Durch die Dynamisierung des Marktumfeldes kommt der kundenzentrierten Softwareentwicklung eine zentrale Rolle zu. Diese tektonische Verschiebung lässt unter Beibehaltung der Strategie der kundenindividuellen Massenproduktion die Komplexität explodieren[6] [6].

Wir müssen daher neue Wege gehen und konsequent datenzentrische Methoden, Prozesse und Werkzeuge in der SDV Entwicklung (Software Defined Vehicle) etablieren. So dürfen relevante Informationen wie Anforderungen aus Regularien oder Architekturentscheidungen nur noch an einer zentralen Stelle im Unternehmen dokumentiert werden. Alle Bereiche, die auf diese Informationen angewiesen sind, können direkt darauf zugreifen. Man spricht hier auch von der „Single Source of Truth“ - also einer völlig unstrittigen Tatsache, die genau an einer Stelle im Unternehmen gefunden werden kann. Diese Informationen müssen konsistent, semantisch korrekt und vollständig sein. Wo immer es sinnvoll ist, sollten Zusammenhänge in einer formalisierten (Maschinen verarbeitbaren) Form und nicht nur in Form von Prosatext beschrieben werden. Die Tatsache, dass sich jede Information und jeder Aspekt entwickeln und verändern kann, muss berücksichtigt werden. Ein konsistentes Versions- und Konfigurationsmanagement ist daher ebenfalls unabdingbar. Diese Anforderungen werden von TPLE erfüllt.

## Die Alternative: Typebased Product Line Engineering (TPLE)

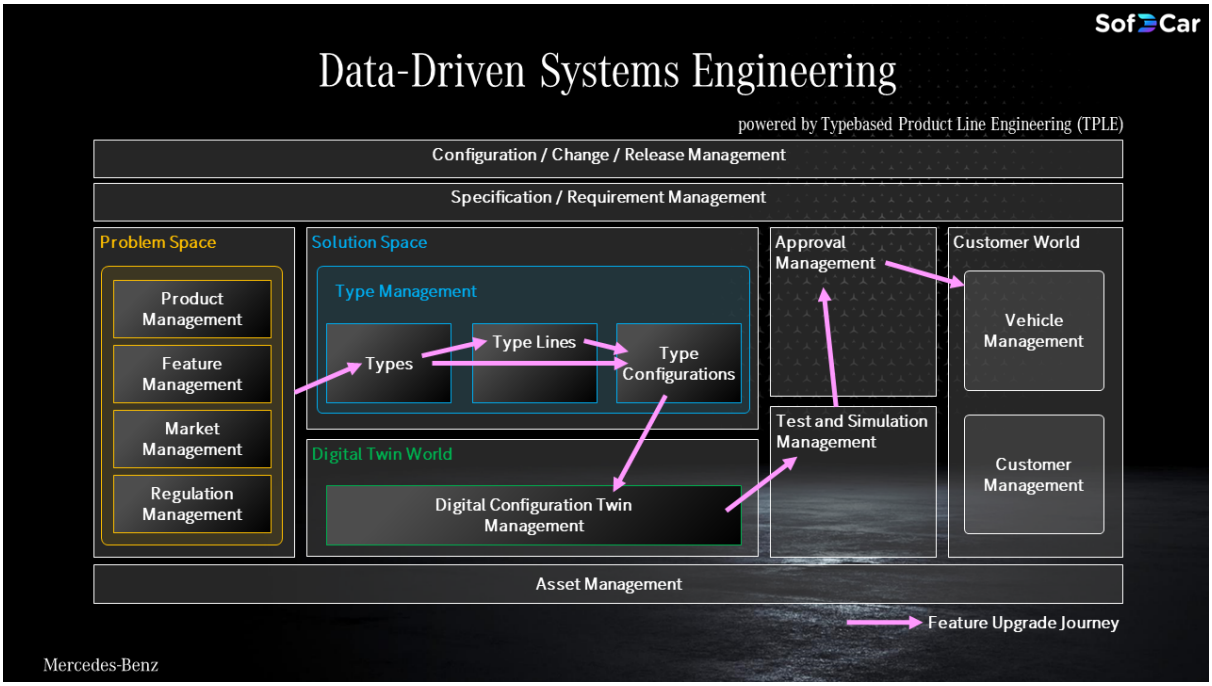



**ABBILDUNG 3: ÜBERBLICK ÜBER TYPEBASED PRODUCTLINE ENGINEERING (TPLE)**

Der Ansatz des Typebased Product Line Engineerings (TPLE) baut auf den aus der Softwarewelt stammenden Konzepten des Product Line Engineerings und der objektorientierten Softwareentwicklung auf und verbindet sie mit dem Paradigma des Systems Engineerings unter Berücksich-

[6] Die Anzahl möglicher Varianten bewegt sich laut einer internen Abschätzung von Mercedes mittlerweile in der Größenordnung von $10^{100}$, was mehr ist als die Anzahl von Atomen im gesamten Universum [8].

tigung der Variantenvielfalt von Produkten aufgrund der Strategie der kundenindividuellen Massenproduktion.

Kernelement von TPLE ist das zentrale TPLE-Datenmodell. Dieser Wissensgraph bildet den Problem- und Lösungsraum einer Produktentwicklung ganzheitlich ab und stellt damit die Basis für ein durchgängiges Varianten- und Konfigurationsmanagement aller für die Produktdokumentation relevanten Aspekte her.

## Was ist ein Wissensgraph?

Das Herzstück eines Wissensgraphen ist sein Wissensmodell: eine Sammlung von miteinander verknüpften Beschreibungen von Konzepten, Entitäten, Beziehungen und Ereignissen. Wissensgraphen kontextualisieren Daten durch Links und semantische Metadaten und bieten einen Rahmen für die Integration, Vereinheitlichung, Analyse und gemeinsame Nutzung von Daten.

## Welche Vorteile hat TPLE?

Die wichtigsten Vorteile von TPLE sind:

- Zentralisierte Datenablage
- Optimierte Zusammenarbeit
- Reduzierter Koordinationsaufwand
- Höhere Qualität in der Entwicklung
    - Schnellere Entwicklung
    - Geringere Entwicklungskosten
    - Automatisches Konfigurationsmanagement
- Einfachere Flotten-Updates
    - Schnellere Fehlerbehebungen
    - Mehr Softwarekorrekturen und weniger Rückrufe
- Erhöhte Transparenz über zum Verkauf stehende und verkaufte Fahrzeuge
    - Höhere Einnahmen durch Upgrades
    - Erlöse für integrierte Funktionen
- Schnellere Anpassung an das Marktumfeld
- Bessere Kundenbindung

Durch die Kombination von Software- und System-Engineering-Methoden ermöglichen wir die folgenden Vorteile:

- Synthese von objektorientierten Methoden und Methoden des Variantenmanagements
- Trennung von Anforderungen (Problemraum) und Lösungen (Lösungsraum)
- Abbildung von generischen Lösungen und Architekturwissen (Typen) und konkreten Lösungskonfigurationen für konkrete Produkte (Typkonfigurationen)
- Abbildung von Varianz durch Vererbungslogik des Typenmodells und durch Optionen innerhalb der Typen möglich
- Durch die Verknüpfung einer Lösungskonfiguration mit einer Feature Konfiguration ist es möglich, direkt die Frage zu beantworten: Was ist der fachliche Kontext dieser Lösungskonfiguration?

## Wie funktioniert TPLE genau?

TPLE dient als zentrales Rückgrat der Produktdokumentation in der Organisation. Jede Abteilung, die an der Produktentwicklung beteiligt ist, hat ihren klaren Berührungspunkt mit einem datenbasierten Integrationsansatz, der die Zusammenarbeit und Prozessautomatisierung auf eine ganz neue Ebene

hebt. Die zugrundeliegenden IT-Systeme werden auf der Basis eines Data Mesh Ansatzes integriert. Jeder Dateneigentümer ist dafür verantwortlich, hochwertige Datenprodukte bereitzustellen, die von anderen Abteilungen auf dezentrale und demokratische Weise genutzt werden können.

Das TPLE-Datenmodell besteht aus zwei Hauptkomponenten:

1. dem Problemraum
2. dem Lösungsraum

Der Problemraum enthält alle wesentlichen Aspekte, die als Input für die Produktentwicklung relevant sind. Die Regelungen der einzelnen Märkte sind über die Märkte mit den entsprechenden Regionen und Ländern verknüpft. Die Features beziehen sich sowohl auf die Vorschriften als auch auf den Markt. Das Produktmanagement schließlich verbindet das Feature Management mit dem Marktmanagement.

Im Lösungsraum bezieht sich das zentrale Type Management sowohl auf das Feature Management als auch auf das Produktmanagement. Die Typen stellen das zentrale Datenobjekt für den Transport von Engineering Wissen dar. Mit den Möglichkeiten zur Modellierung von Schnittstellen, Zustandsautomaten, Funktionen, Optionen und Komponententypen, ergänzt durch Vererbung, steht ein breites Spektrum an Modellierungswerkzeugen zur Verfügung. Type Lines (oder manchmal auch Partial Type Configurations genannt) sind ein Zwischenschritt, um Typen mit einigen konkreten Optionswerten zu instanziieren, während andere Optionen noch undefiniert sind, um in diesem Stadium eine gewisse Varianz zu erhalten. Eine konkrete Typkonfiguration kann erstellt werden, wenn alle Optionen vollständig definiert sind. Diese Typkonfigurationen sind die Entwürfe für die konkreten Produktinstanzen, die dann auf der Grundlage dieser Entwürfe erstellt werden.

## TPLE-Datenbank für Cyber Security Fragen

Der untersuchte Security Fall basiert auf einem realen Angriff. Im folgenden Teil wird der Fall allerdings abstrahiert und weitere Details werden hypothetisch betrachtet. Daher werden die zwei Baureihen eines OEMs generisch als „Baureihe B“ und „Baureihe C“ bezeichnet.

### Was sind die gemeinsamen Features der betroffenen Fahrzeuge?

Wie bereits erwähnt, stellt ein bestimmter Aspekt der E/E-Architektur der Fahrzeuge das für den Security Vorfall relevante Feature dar. Dieser kann in der TPLE-Datenbank als Konfiguration gespeichert werden. Wenn die Ursache noch nicht bekannt ist, aber mehrere Fahrzeuge als gestohlen identifiziert wurden, ermöglicht TPLE die Anwendung von Graphanalysemethoden, um automatisch den maximalen gemeinsamen Teilgraphen zu bestimmen, was die Suche nach dem Angriffsvektor erheblich vereinfacht.

### Welche anderen Fahrzeuge verfügen über die gleichen oder ähnliche Features und sind daher ebenfalls anfällig für diesen Angriff?

Um diese Frage zu beantworten, müssen wir die Varianz der E/E-Architekturen und der Konfigurationen der bordeigenen Steuergeräte im Portfolio der Fahrzeuglinien und Fahrzeugliniенderivate der OEM-Marke untersuchen. Hier kann eine Abfrage in der TPLE-Datenbank aufschlussreiche Ergebnisse liefern.

Die E/E-Architektur Konfiguration der Baureihe B und Baureihe C sieht so aus:

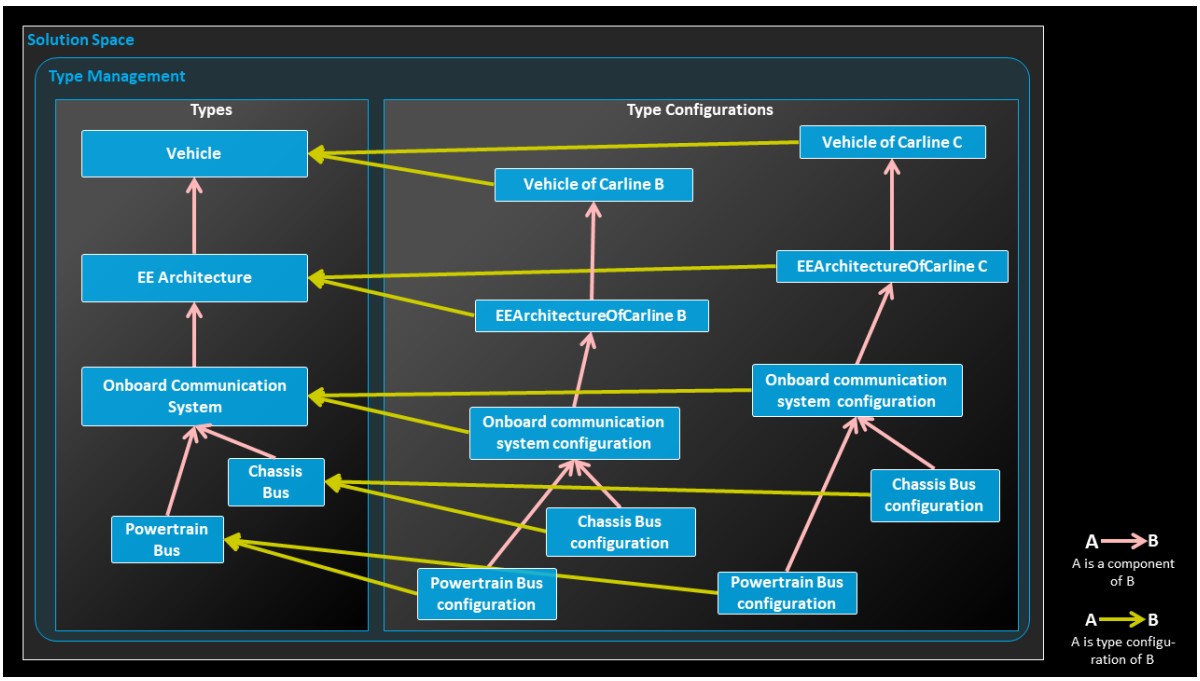



**ABBILDUNG 4: DIE E/E-ARCHITEKTUR-KONFIGURATION DER BAUREIHE B UND DER BAUREIHE C**

Die Kästchen im Bereich Typen stellen Typen aus der Typbibliothek auf einer sehr hohen Ebene dar. Der Typ „Fahrzeug“ enthält eine Komponente, die vom Typ „EE-Architektur“ ist. Diese enthält das „Onboard Communication System“ und so weiter.

Die Kästchen im Bereich „Typkonfigurationen“ stellen konkrete Instanziierungen der Typen dar. So enthält das „Fahrzeug von Carline B“ eine Instanz namens „EEArchitectureOfCarline B“ vom Typ „EE Architecture“. Wie in Abb. 4 dargestellt, könnte es E/E-Architekturen anderer Modelle geben (z. B. Baureihe C), die dieselbe Konfiguration des Onboard-Kommunikationssystems verwenden wie Baureihe B. Dies bedeutet, dass sie auch dieselben Konfigurationen des Chassis Bus und des Powertrain Bus enthalten. Folglich wäre in diesem hypothetischen Beispiel auch die Baureihe C von diesem Sicherheitsproblem betroffen und sollte bei der Entwicklung von Gegenmaßnahmen ebenfalls berücksichtigt werden.

### Wie können diese anfälligen Fahrzeuge schnell davor geschützt werden, Opfer eines solchen Angriffs zu werden?

Die Ausarbeitung eines Sicherheitspatches ist eine Aufgabe, die von Experten ausgeführt werden muss. In einigen Fällen kann das CSMS Hinweise geben, wie z. B. die Auflistung verwundbarer Softwarebibliotheken. Im Falle des schlüssellosen Fahrzeugdiebstahls wäre die schnellste Option jedoch die Aktualisierung des CAN-Gateways. Dies wird nicht durch eine automatische Analyse angezeigt, kann aber in Betracht gezogen werden, sobald der relevante Teil der E/E-Architektur identifiziert wurde.

### Gibt es Maßnahmen, die bei bereits erfolgreich angegriffenen und gestohlenen Fahrzeugen angewendet werden können? Ist es zum Beispiel möglich, das Fahrzeug sicher außer Betrieb zu nehmen?

Sind die gestohlenen Fahrzeuge identifiziert, kann diese Frage in der Regel durch eine Abfrage der Feature Konfiguration dieser Fahrzeuge beantwortet werden.

### Welche Software- und Hardware-Abhängigkeiten bestehen für die verschiedenen Typen von bedrohten Fahrzeugen, die beim Entwurf eines Sicherheitspatches berücksichtigt werden müssen?

TPLE kann die erforderlichen Informationen liefern, da es ein Single Point of Truth ist.

### Wie kann der Sicherheitspatch an alle gefährdeten Fahrzeuge verteilt werden?

Wie bereits erwähnt, kann dies beispielsweise durch Over-the-Air-Updates (OTA-Updates) erfolgen. Diese können jedoch nur durchgeführt werden, wenn diese Funktion in den gefährdeten Fahrzeugen verfügbar ist, was wir ebenfalls durch eine Abfrage der TPLE-Datenbank herausfinden können.

### Welche Verallgemeinerungen oder Varianten des Angriffs könnten in Zukunft auftreten, und welche Auswirkungen hätten diese auf die Fahrzeuge?

Diese Frage impliziert mehrere Unterfragen, zu deren Beantwortung die TPLE-Datenbank beiträgt:

- Gibt es weitere Busse in den Fahrzeugen, die von außen zugänglich sein könnten?
- Gibt es andere E/E-Konfigurationen mit nicht authentifizierter Smart Key Kommunikation?
- Gibt es andere potenziell verwundbare Kommunikationsschnittstellen?
- …

Zur Beantwortung dieser Fragen können auch Graph-Analyse-Werkzeuge hilfreich sein, um Ähnlichkeiten zwischen verschiedenen Fahrzeugkonfigurationen abzuschätzen.

### Welche langfristigen Maßnahmen können ergriffen werden, um künftige Angriffe zu verhindern, und sind diese für die Typgenehmigung relevant?

Eine Möglichkeit ist die Einführung einer sicheren Onboard-Kommunikation (SecOC) für das Türsteuergerät, das Smart Key Steuergerät und das Motorsteuergerät, wenn diese Steuergeräte SecOC-fähig sind. Diese Information kann wiederum durch eine Abfrage der TPLE-Datenbank in Erfahrung gebracht werden. Im folgenden hypothetischen Beispiel kommen wir zu dem Ergebnis, dass bei der Carline B mit Modelljahr 2021 das Schlüsselsteuergerät nicht auf SecOC aufgerüstet werden kann, während dies bei der Carline B ab Modelljahr 2022 möglich ist.

Baureihe B Modelljahr 2021 vs. Modelljahr 2022

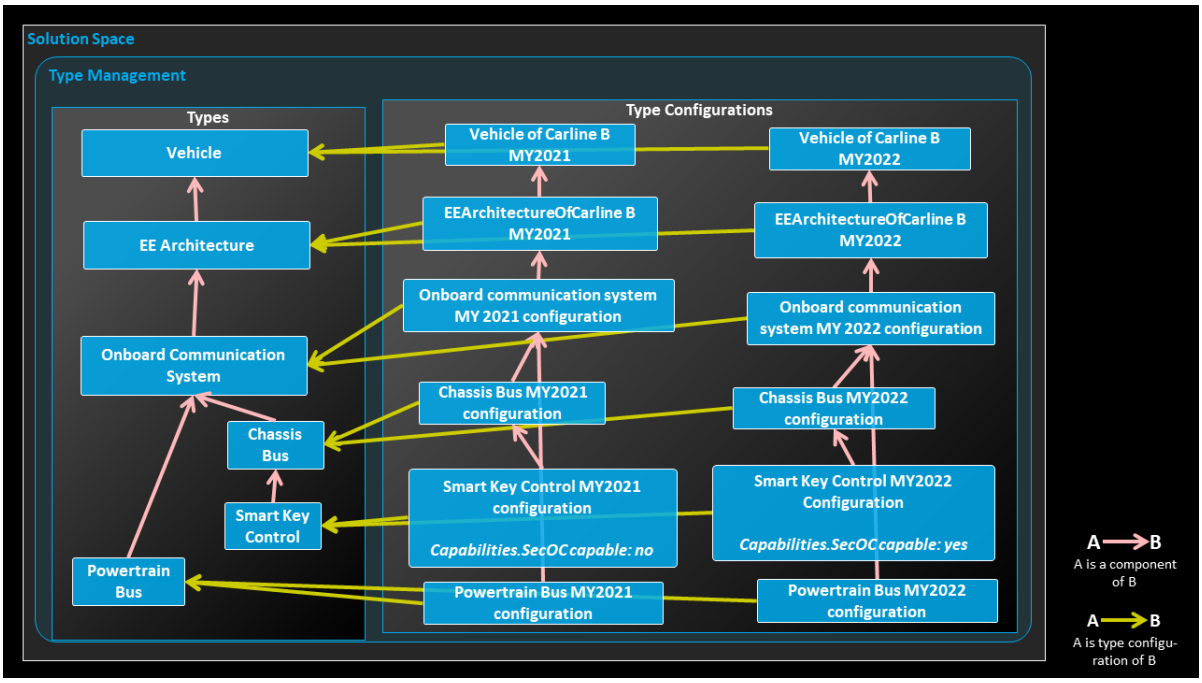


ABBILDUNG 5: DIE BEIDEN E/E-ARCHITEKTUREN VON CARLINE B MODELLJAHR 2021 UND MODELLJAHR 2022.

### SIND DIE VORZUNEHMENDEN ÄNDERUNGEN FÜR DIE TYPGENEHMIGUNG RELEVANT?

In diesem Fall können wir von der Tatsache profitieren, dass TPLE auch den Problemraum modelliert, der alle für die verschiedenen Fahrzeugvarianten relevanten Vorschriften enthält. Dies legt nahe, dass z.B. bei einem Upgrade des Motorsteuergeräts ein Homologationsprozess durchgeführt werden muss.

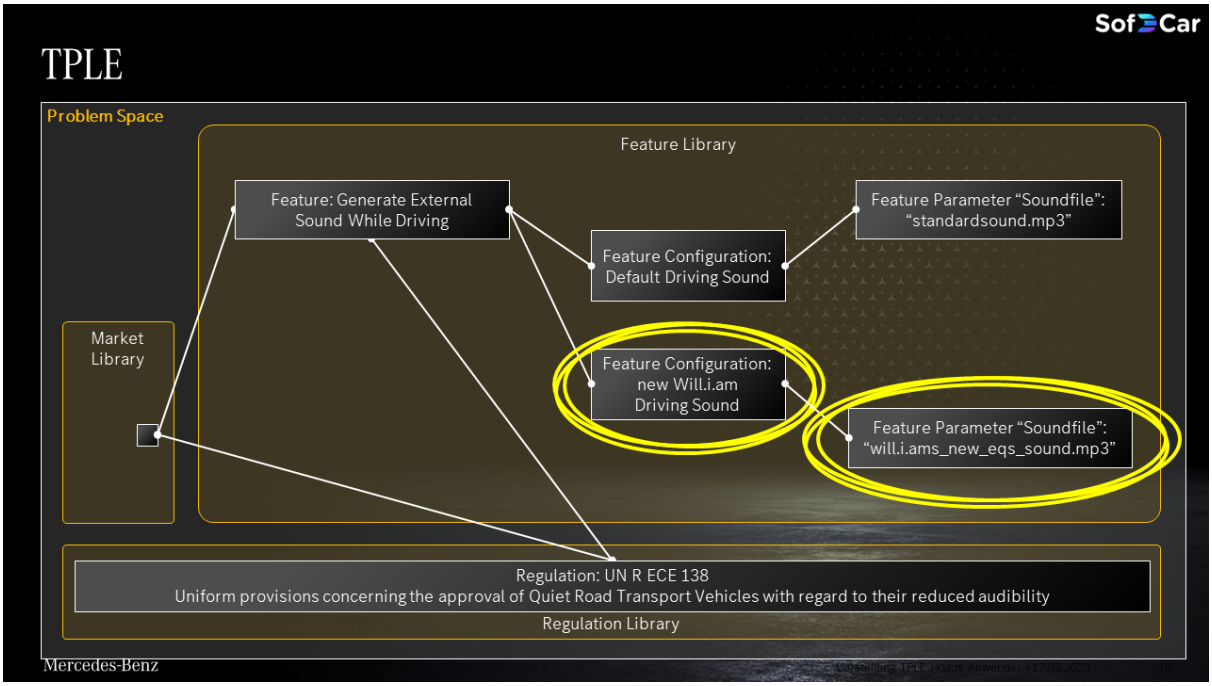



ABBILDUNG 6: DIE ABHÄNGIGKEIT ZWISCHEN FEATURES UND VORSCHRIFTEN

Wie in Abb. 6 in einem anderen Fall „Software-Update des akustischen Fahrzeugwarnsystems (AVAS)“ dargestellt: Sobald die Feature-Konfiguration geändert wird, führt die Abhängigkeit von der Regularie UN R ECE 138 dazu, dass ein automatisch eingeleiteter Homologationsprozess durchgeführt werden muss. Weitere Details zu diesem Fall sind als einfacher Homologations-Anwendungsfall AVAS in [7] beschrieben.

### WELCHE KONKRETEN FAHRZEUGINSTANZEN (VINS) SOLLEN WELCHES UPDATE ERHALTEN?

Neben der E/E-Architektur hängt die Kompatibilität auch von den Software- und Hardware-Konfigurationen der einzelnen Fahrzeuge ab. Nachdem mit Hilfe der TPLE-Datenbank geeignete Konfigurationen ermittelt wurden, können in Verbindung mit der zentralen Fahrzeugdatenbank konkrete Fahrzeuginstanzen und Update-Wege identifiziert werden.

## ERGEBNISSE

Bei der Untersuchung der Anwendung von TPLE auf den Angriff des schlüssellosen Fahrzeugdiebstahls haben wir festgestellt, dass die Einführung von TPLE für solche Sicherheitsuntersuchungen und die Festlegung geeigneter Abhilfemaßnahmen von großem Nutzen ist. Von den 10 relevanten Fragen, die zu Beginn des Papiers gestellt wurden, werden die Antworten auf 9 von ihnen durch TPLE wesentlich erleichtert. Lediglich bei der Frage nach den geeigneten Gegenmaßnahmen kann TPLE nicht unterstützen, wohl aber bei der Frage nach ihrer Umsetzbarkeit. Einer der Hauptvorteile von TPLE ist die Geschwindigkeit, mit der Erkenntnisse gewonnen werden können, was absolut notwendig ist, um mit dem schnellen Auftreten neuer Sicherheitsvorfälle Schritt zu halten. Darüber hinaus bietet es eine Möglichkeit, alle relevanten Fahrzeugvarianten schnell zu identifizieren und alle gewonnenen Erkenntnisse in einer zentralen Datenbank zu speichern (da es sich um einen Single Point of Truth handelt). Nicht zuletzt bietet es die Möglichkeit, einzelne Analyseschritte zu automatisieren, was die

Arbeitsbelastung der Sicherheitsanalysten reduziert, Prozesse beschleunigt, die Zuverlässigkeit von Sicherheitsuntersuchungen und Abhilfemaßnahmen erhöht und damit letztlich zu einer höheren Kundenzufriedenheit beiträgt.

## AUSBLICK

Da die Einführung von TPLE eine grundlegende und disruptive Veränderung der technischen Prozesse erfordert, haben große Organisationen wie OEMs, Tier 1 und Tier 2 mit dieser Herausforderung zu kämpfen. Es ist nicht nur eine technische Frage und daher mit Geld und Zeit zu bewältigen, sondern es ist eher ein Mentalitätsthema.


**ABBILDUNG 7: QUELLE: GEORGE COUROS: WHO WANTS TO CHANGE?**

Um eine zentrale TPLE-Engineering-Wissensbasis zu schaffen, muss eine komplette Dateninfrastruktur aufgebaut werden, alle relevanten Daten aus den verschiedenen Silos müssen (möglichst automatisiert) integriert werden, und viele Prozesse, Methoden und Werkzeuge müssen geändert werden, um der Organisation einen Mehrwert zu bringen.

## DER WEG AUS DEM DILEMMA

Die Frage ist nun: Wie kann man einen Ausweg aus diesem Dilemma finden?

1. Zuallererst braucht ein solches Unterfangen Unterstützung aus dem Top-Management. Dadurch wird gewährleistet, dass Hindernisse aus dem Weg geräumt werden, die sich bei der Umsetzung des Wandels ergeben.
2. Zunächst sollte mit einem kleinen, gut messbaren und erklärbaren Anwendungsfall begonnen werden, der einen Mehrwert für das Unternehmen darstellt.
   Ein Anwendungsfall aus dem Bereich der Cybersicherheit wie hier beschrieben stellt einen guten Fall dar, da bei einem Security Vorfall Schnelligkeit oberste Priorität hat und Zeit sich sehr gut messen lässt.
3. Aufbau einer Dateninfrastruktur unter Verwendung des Data-Mesh-Paradigmas, um Synergien zu schaffen, wenn immer mehr Anwendungsfälle hinzugefügt werden.
4. Aufbau eines weitgehend automatisierten Prozesses zur Übernahme vorhandener Daten aus den aktuellen inhomogenen und dezentralen Quellen.

Dieses Whitepaper ist im Rahmen des öffentlich geförderten Forschungsprojekts Software-Defined Car entstanden. Wir planen, das TPLE-Datenmodell in die Open-Source-Gemeinschaft einzubringen, da wir glauben, dass dies der einzige Weg ist, um ein nicht-diskriminierendes Systems-Engineering-Ökosystem zu schaffen, das unabhängig von proprietären Datenformaten und unabhängig von jedem Tool-Anbieter ist. Diese Transparenz bringt zusätzliche Vorteile in Bezug auf die Sicherheit.

# REFERENZEN

[1] K. Tindell, „CTO blog," CANIS Automotive Labs, 03 04 2023. [Online]. Available: https://kentindell.github.io/2023/04/03/can-injection/. [Zugriff am 30 10 2024].

[2] L. Sommerfeld, „driving.ca," 4 09 2023. [Online]. Available: https://driving.ca/column/lorraine/auto-insurance-surcharge-theft-appeal. [Zugriff am 30 10 2024].

[3] ISO, „ISO/SAE 21434:2021," 2021. [Online]. Available: https://www.iso.org/standard/70918.html. [Zugriff am 30 10 2024].

[4] UNECE, „UN Regulation No. 155 - Cyber security and cyber security management system," 2021. [Online]. Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security. [Zugriff am 9 May 2023].

[5] ISO, „ISO/IEC 26580:2021," 2021. [Online]. Available: https://www.iso.org/standard/43139.html. [Zugriff am 30 10 2024].

[6] A. Kübler, C. Zengler und W. Küchlin, „Model Counting in Product Configuration," *Electronic Proceedings in Theoretical Computer Science,* Bd. 29, p. 44–53, 2010.

[7] Bosch, ETAS, Certivity, TÜV Rheinland, T-Systems, Ferdinand-Steinbeis-Institut, NIO, Hochschule Heilbronn , „Whitepaper: Continuous Homologation for Software-defined Vehicles," 04 10 2024. [Online]. Available: https://www.digital.auto/_files/ugd/604381_8407b82ac15a4ae0a0ed508894bcf814.pdf. [Zugriff am 30 10 2024].

[8] B. M. Deiss, „Astronomie: Wie viele Atome gibt es im Universum," SWR, 2024. [Online]. Available: https://www.swr.de/wissen/1000-antworten/wie-viele-atome-gibt-es-im-universum-100.html. [Zugriff am 06 11 2024].

# ACKNOWLEDGMENTS

Gefördert vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages