Automotive SW: Vertikalisierung versus Horizontalisierung

Die (R)Evolution der Automotive SW schreitet voran

Dr.-Ing. Detlef Zerfowski, ETAS GmbH

1. Rückblick auf die „(R)Evolution“ im letzten Jahr

In dem auf dem ESE-Kongress 2017 vorgestellten Artikel „(R)Evolution der Automotive-Software-Architekturen. Wie neue Software-Technologien die Automobilindustrie verändern“ [2], wurde über die Auslöser der revolutionären Änderungen in der Automobil-SW-Industrie berichtet. Die in dem Artikel beschriebenen Tendenzen haben sich im vergangenen Jahr bestätigt. Die Revolution der Automobil-SW-Industrie schreitet weiter voran.

Die Industrie kämpft weiterhin mit den Veränderungen und den einhergehenden Herausforderungen. Zum einen stellt der Übergang von µ-Controller basierten, klassischen embedded Steuergeräten hin zu µ-Prozessor basierten bzw. Cloud basierten Lösungen die entwickelnde Bereiche vor enorme Herausforderungen, z.B. wie die Kompetenzprofile der Software-Engineering-Bereiche zu ändern bzw. zu erweitern sind.

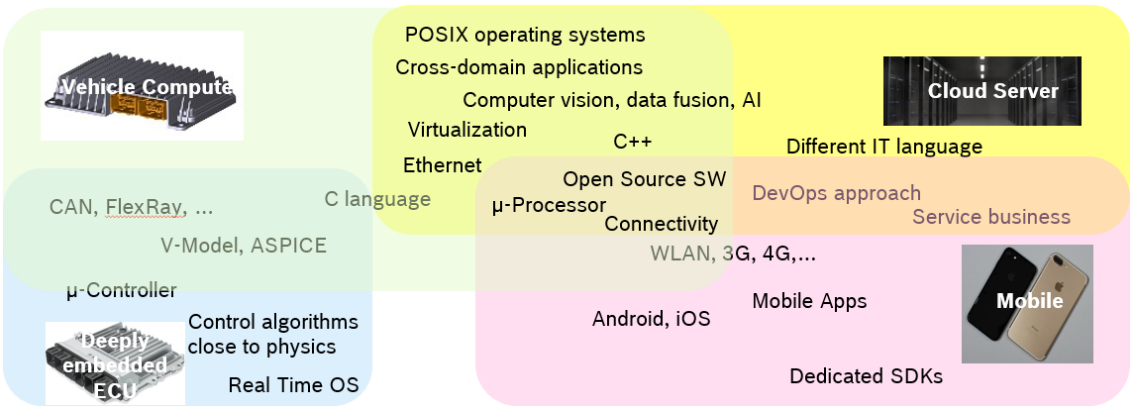

Abbildung 1: SW ≠ SW - Unterschiedliche Arten von Software dringen in die Automotive Domäne ein.

In Abbildung 1 [2] wird die Veränderung der benötigten Softwareprofile deutlich. Die stark durch signalbasierte Regelungsalgorithmen geprägte Software der „Deeply Embedded ECUs“ ist durch harte Realzeitanforderungen, Automotive SPICE (ASPICE), Entwicklung nach V-Model etc. charakterisiert.
Neue sich in Entwicklung befindlicher Fahrzeugrechner bauen auf völlig anderen aus der IT-Welt stammenden Betriebssytemen auf und führen neue SW-Engineering-Paradigmen in die Automobilindustrie ein. Die klassische Lastenheft-getriebene Komponentenentwicklung ändert sich bei Fahrzeugrechner immer stärker zu einer Separierung von SW und HW.

Zusätzlich drängen zunehmend Anwendungen aus den Smartphone Eco-Systemen ins Fahrzeug (Abbildung 1 unten rechts).

Der technologischen Wandel in der Automobil-Software kommt gepaart mit organisatorischen Veränderungen, um die Herausforderungen adäquat adressieren zu können.

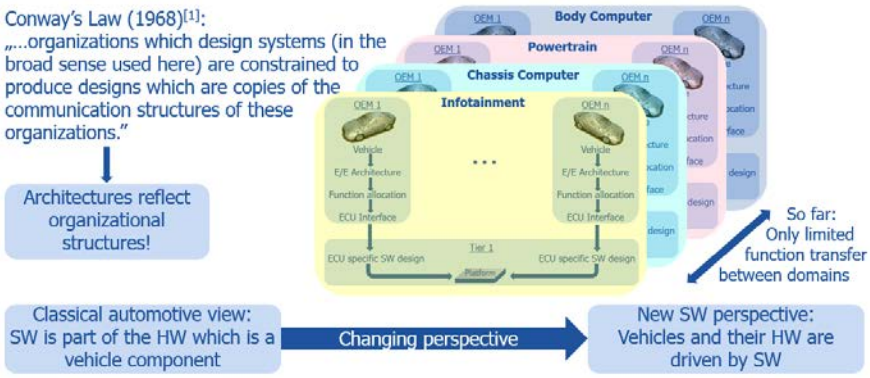

Abbildung 2: Conway's Law trifft die Automobilindustrie.

Wie bereits in [2] ausgeführt, sind wir hier mit einem Fall von „Conway's Law" [1] konfrontiert:
„…organizations which design systems (in the broad sense used here) are constrained to produce designs which are copies of the communication structures of these organizations."
Das heißt, Produkte und deren Architekturen folgen den Organisationsstrukturen. Das bisherige Steuergerätekomponenten-orientierte embedded ECU-Geschäft ist dabei vertikal vom OEM bis zu den Zulieferern durchorganisiert. Beispiele hierfür sind die seit langem etablierten Zuordnungen von Funktionen auf dedizierte Steuergeräte, die wiederum in den seit Langem etablierten Domänen und Organisationen angesiedelt sind.

2. Vom µ-Controller mit klassischem AUTOSAR zum µ-Prozessor mit AUTOSAR adaptive

Die zuvor beschriebene embedded Entwicklung erfolgt stark vertikalisiert. Die Ziel-Hardware legt die maximal verfügbaren Ressourcen fest, die über zeitscheibenorientierte Realzeitbetriebssysteme, die raren Rechnerressourcen den SW-Funktionalitäten zur Verfügung stellen. Auch die Kommunikationsstrukturen zwischen den unterschiedlichen Komponenten im Fahrzeug sind sehr stark eingeschränkt. Zentrale Designelemente sind statisch vorgegebene CAN-Matrizen, die bereits zur Entwicklungszeit festlegen, welche Botschaft in welchem Zeitraster an wen gesendet wird.

Auch auf höherer Funktionsebene ist diese Struktur erkennbar. Einmalig an Steuergeräte zugewiesene Funktionen lassen sich später nicht, bzw. nur mit sehr hohen Aufwänden über Steuergerätegrenzen hinweg verschieben.

Ein wesentlicher Vorteil dieses Ansatzes liegt andererseits im erzwungenen Determinismus des Steuergeräteverhaltens und die hierdurch leichter zu beherrschenden Safety-Anforderungen. Gleichzeitig behindert dieses Design jedoch die Einführung moderner, aus der IT-Industrie kommender SW-Technologien.

Natürlich wurden auch im deeply embedded Bereich Horizontalisierungsaspekte vorangetrieben. Als Beispiele seien hier Diagnose-Standards und AUTOSAR genannt. Aber auch in diesem Kontext gilt: Es handelt sich um einen zentral definierten Standard für Basis SW Stacks für µ-Controller ECUs, der sich über viele Jahre hinweg entwickelt hat. Der Ansatz war, einen möglichst hohen Gleichanteil an hardwarenaher und applikationsunabhängiger Basis SW zu Standardisierung. Im laufenden Betrieb ist damit eine Horizontalisierung von Funktionen jedoch nicht sichtbar.

Mit den aufkommenden µ-Prozessor-basierten Fahrzeugrechnern ändert sich die Situation grundlegend.

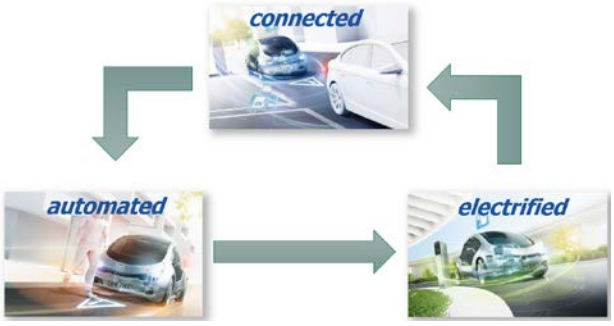

Abbildung 3: Konnektivität, automatisiertes Fahren und Elektrifizierung verändern den Automobilsektor.

Durch die aktuellen Markanforderungen bzgl. Konnektivität, automatisiertes Fahren, Elektrifizierung (Abbildung 3) und neue Eigentümerkonzepte für Fahrzeuge ergeben sich massive Verschiebungen von Funktionalitäten zwischen den im Fahrzeug vorhandenen Rechnerknoten, sowie gänzlich neuer Funktionen, die auf µC-basierten Systemen effizient nicht darstellbar sind.

An dieser Stelle kommt der neue Standard AUTOSAR Adaptive zum Einsatz. Dieser auf µP-Systeme ausgerichtete Standard unterstützt z.B. dynamische SW-Änderungen, hoch-parallele Architekturen und Service-orientierte Kommunikation. Mit diesen Ansätzen werden µP-basierte Rechnern, neben den bereits existierenden Infotainment-Anwendungen nun auch für Funktionen mit höheren Safety-Anforderungen als im Infotainment-Umfeld geöffnet (Abbildung 4).

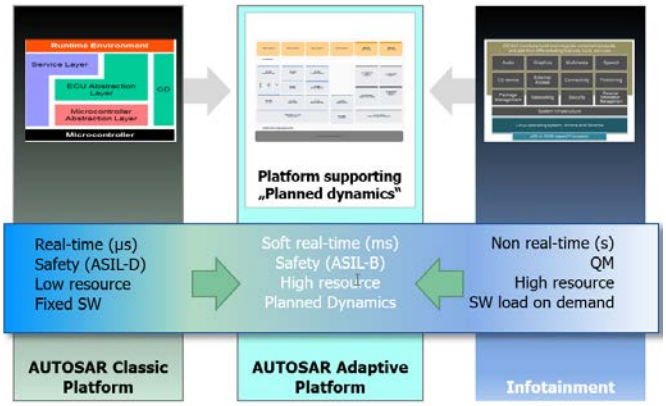

Abbildung 4: AUTOSAR Adaptive schließt die Lücke zwischen klassischem AUTOSAR und Infotainment.

Auf Grund des dramatischen Anstiegs der verfügbaren Rechnerressourcen (z.B. mehr als 1000facher Speicher) beim Übergang von µC- zu µP-Systemen müssen andere Basis SW Systeme und Entwicklungsmethoden verwendet werden. Der Einsatz von aus der Konsumerelektronik stammenden POSIX Betriebssystemen ist ein absolutes Muss.
Hierbei ist zu bemerken, dass es nicht das Ziel ist, dass AUTOSAR Adaptiv das klassische AUTOSAR ablösen wird. Beide Systeme werden in Fahrzeugen koexistieren (Abbildung 5), da für realzeitkritische Anwendungen reine µP-Systeme nicht geeignet sind. Schätzungen gehen davon aus, dass weniger als 10% der im Fahrzeug verbauten Steuergeräte µP-basierte Fahrzeugrechner sein werden, diese werden jedoch den bei weitem größtem Anteil der Fahrzeugsoftware tragen.
Damit ist die Grundlage für eine stärkere Horizontalisierung der SW innerhalb des Fahrzeuges gelegt. Die Entkopplung der SW von der HW durch Verwendung Service orientierter Architekturen unterstützt einen deutlich modularisierteren Aufbau darüber liegender SW-Schichten.

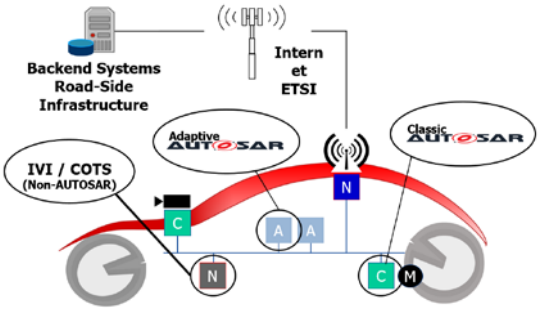

Abbildung 5: AUTOSAR Adaptive und klassisches AUTOSAR bleiben parallel im Fahrzeug.

3. Horizontalisierung am Beispiel Security

Das Thema der steigenden Horizontalisierung lässt sich in diesem Zusammenhang am Beispiel Security verdeutlichen. In der Vergangenheit waren Fahrzeuge „implizit" durch die Fahrzeuggrenzen geschützt. Um unberechtigten Zugang im Fahrzeugnetzwerk zu

erlangen, war der physikalische Zugriff auf das Fahrzeug notwendig. Entsprechend konnte nur das konkret attackierte Fahrzeug manipuliert werden.
Mit der zunehmenden Konnektivität verändert sich der Angriffsvektor vollständig (Abbildung 6). Der physikalische Zugriff auf das Fahrzeug ist nicht mehr zwingend erforderlich und bei einem erfolgreichen Angriff ist potentiell eine große Menge an Fahrzeugen unmittelbar betroffen.

Um dieser Situation zu begegnen, müssen Sicherheitskonzepte und –lösungen etabliert werden, die nicht an ECU-Grenzen haltmachen. Mehrstufige Sicherheitskonzepte sind erforderlich. Diese können auch nicht auf Teile der in den Steuergeräten verwendeten Software begrenzt sein. So stellen die aktuellen Security-Anforderungen im klassischen AUTOSAR einen wichtigen Baustein dar, sind aber nicht ausreichend wenn es darum geht Security-Anforderungen zwischen AUTOSAR basierten und anderen Steuergeräten und Fahrzeugrechnern sicherzustellen. Dabei sind ganzheitliche Ansätze erforderlich, wie sie die ETAS Tochter ESCRYPT bereitstellt. Das ETAS bereits vor mehreren Jahren ein eigenes Unternehmen für Automotive-Security am Markt etabliert hat, verdeutlicht die Notwendigkeit für die Horizontalisierung des Themengebietes Security.

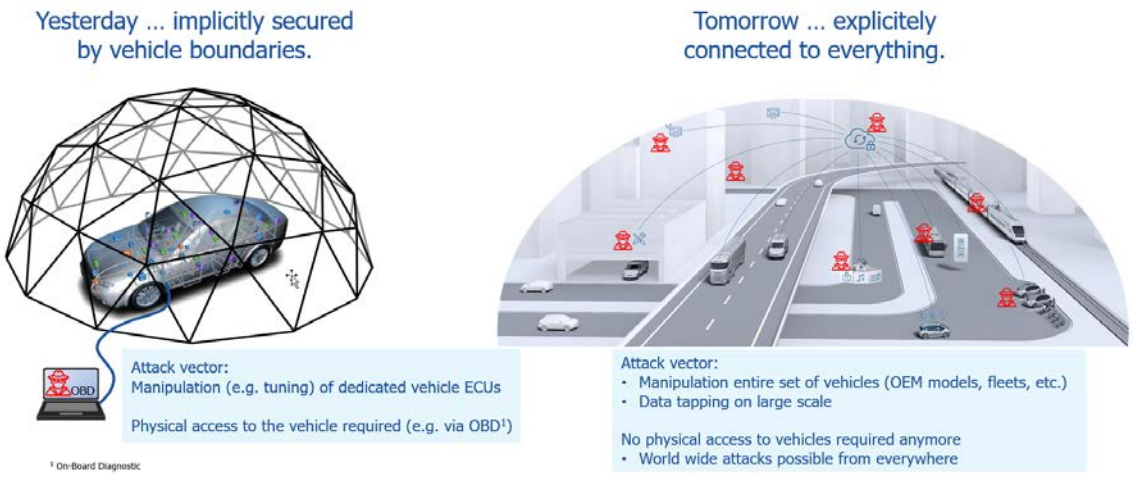

Abbildung 6: Security-Angriffsvektoren verändern sich.

Mit der Einführung der Fahrzeugrechner müssen folgende Herausforderungen adressiert werden:

- Deutlich mehr potentielle Einfalltüren für Angreifer müssen abgesichert werden.
- Dynamische Kommunikationsinfrastrukturen erfordern den Einsatz von Security-Maßnahmen aus der IT-Industrie.
- Die Integrität von sich in der E/E-Architektur dynamisch verändernder Software muss sichergestellt werden.
- Security-Maßnahmen müssen etabliert werden, die cross-ECU und über Fahrzeuggrenzen hinweg wirken.
- Security-Updates müssen über die Luftschnittstelle über den Lebenszyklus des Fahrzeugs bereitstehen.

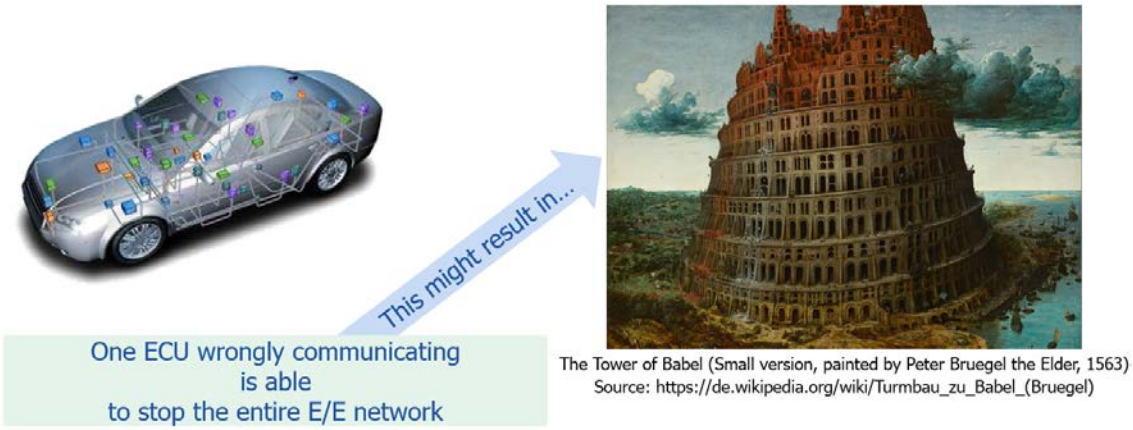

Abbildung 7: Auswirkung wenn Security nicht funktioniert.

Bei all diesen Herausforderungen muss sichergestellt werden, dass alle im Fahrzeug verbauten Komponenten und deren Schnittstellen nach außen einwandfrei aus Security-Sicht funktionieren. Ein einzelnes Steuergerät kann bei einer fehlerhaften Kommunikation das ganze E/E-Netzwerk lahmlegen (Abbildung 7).
Hieraus ergibt sich zwingend, dass Security kein Steuergeräte-spezifisches Thema ist, sondern sich über deren Grenzen hinweg, über das gesamte Fahrzeug, bis in Fertigungsabläufe beim OEM und Tier1 auswirkt.

4. RTA-VRTE und AUTOSAR Adaptive

Wie bereits weiter oben erwähnt, stellt AUTOSAR Adaptive einen zentralen Baustein für Fahrzeugrechner dar und wird die Horizontalisierung der SW im Fahrzeug weiter vorantreiben. Dabei wurde nur eine Instanz einer AUTOSAR Adaptive auf einem Fahrzeugrechner betrachtet. Solange auf einem Fahrzeugrechner nur eine einzelne Anwendungsdomäne abläuft, ist der Einsatz einer AUTOSAR Adaptive SW mit geeignetem POSIX Betriebssystem als Basis SW möglicherweise ausreichend.
Bezüglich der Anforderungen aus zukünftigen E/E-Architekturen ist AUTOSAR Adaptive ein erster notwendiger, aber nicht ausreichender Schritt.
Zukünftige Fahrzeugrechner, die als Integrationsplattformen für SW-Funktionen aus unterschiedlichen Bereichen, mit unterschiedlichen ASIL-Anforderungen stammen, benötigen Plattformen, die diesen unterschiedlichen Safety-Anforderungen genüge tragen.
Es werden flexible Plattformen benötigt, die über gemischte µC-µP-Systeme unter Verwendung von Hypervisor-Technologien und damit über das klassische AUTOSAR und AUTOSAR Adaptive skalieren (Abbildung 8).

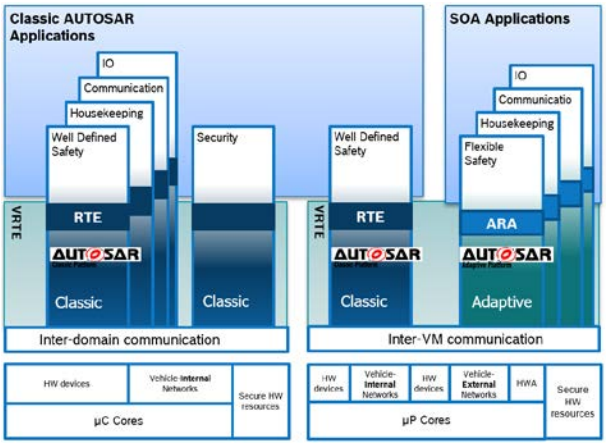

Abbildung 8: VRTE jenseits von AUTOSAR Adaptive.

Des Weiteren wird die Unterstützung von Hypervisor-Lösungen benötigt, auf denen gemischte ASIL-Anwendungen mit unterschiedlichen Betriebssystemen auf demselben Fahrzeugrechner laufen. Dies erzwingt entsprechende Plattformkonzepte um sowohl Safety- und Security-Anforderungen (z.B. Freedom from Interference) zu erfüllen.
Aus diesem Grund entwickeln BOSCH und ETAS die RTA-VRTE (Real-Time-Application Vehicle Run Time Environment), welche AUTOSAR Adaptive konform ist und zusätzliche, cross-ECU relevante Plattformfunktionen bereitstellt. Dabei wird besonderes Augenmerk auf ein offenes, flexibles Framework gelegt, so dass eine einfache Integration von 3rd-Party-SW unterstützt wird.

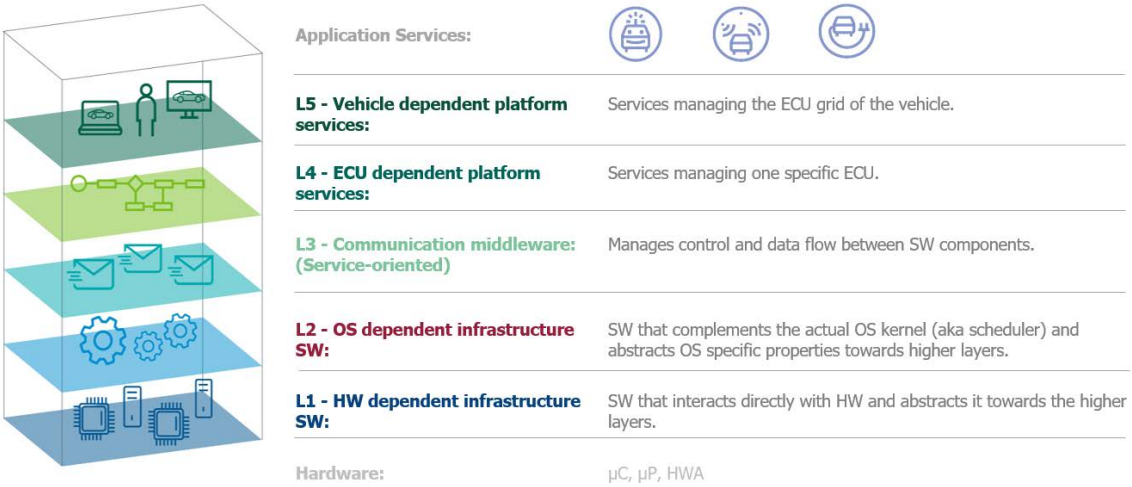

Abbildung 9: Unterschiedliche Software-Ebenen (L1 bis L5) adressiert durch die VRTE.

Die VRTE stellt somit ein weiteres Beispiel für die SW-Horizontalisierung im Automobil-Sektor dar. Zukünftige Fahrzeugrechner werden somit aus einer Menge horizontaler SW-Anteile, sowie vertikaler SW-Anteile innerhalb der Anwendungsdomänen aufgebaut sein. Hieraus ergibt sich eine Aufteilung und

Verschiebung von Verantwortlichkeiten bis hin zu organisatorischen Änderungen, um den Auswirkungen von Conway's Law entgegenzuwirken.

5. Zusammenfassung

Mit dem Einzug der µ-Prozessor-basierten Fahrzeugrechnern setzt sich die Separierung der SW von der HW fort. Gleichzeitig wird eine deutlich stärkere Separierung der Software in horizontale und vertikale Anteile auftreten, die auch zu organisatorischen Änderungen in Unternehmen der Automobilindustrie führen.

Abkürzungsverzeichnis

HW	Hardware
SW	Software
ECU	Electronic Control Unit (Elektronisches Steuergerät)
ASPICE	Automotive SPICE: Aus dem ISO Standard ISO/IEC 15504 (SPICE) abgeleitetes Automotive-spezifisches Reifegradmodel zur Bewertung der Steuergeräteentwicklung in der Automobilindustrie.
POSIX	Portable Operating System Interface: Ein Satz von IEEE Standards der Application Programming Interface (API) für POSIX kompatible Betriesbssysteme definiert.
RTA-VRTE	Real Time Application – Vehicle Run Time Environment. BOSCH/ETAS Produkt für gemischte ASIL-Anwendungen auf Fahrzeugrechnern

Abbildungsverzeichnis

Literaturverzeichnis

[1] Conway, Melvin E. (1968): How do committees invent?
http://www.melconway.com/Home/Conways_Law.html
[2] Detlef Zerfowski, S K Niranjan: „(R)Evolution der Automotive-Software-Architekturen. Wie neue Software-Technologien die Automobilindustrie verändern.” Tagungsband Embedded Software Engineering Kongress 2017, Sindelfingen, 4.-8. Dezember 2017, Seiten 411-424

Autor

Dr.-Ing. Detlef Zerfowski (Vice President, ETAS GmbH) wechselte nach seiner Promotion in der Informatik (TH Karlsruhe) im Bereich medizinischer Signalverarbeitung zur Robert Bosch GmbH. Seine 18-jährige Automotive-Erfahrung deckt die Embedded SW-Entwicklung in verschiedenen Domänen (Body Electronics, Bremssysteme, Park Assistenten) ab.
Von 2009-2012 baute Herr Zerfowski für den Geschäftsbereich Automotive Electronic einen Entwicklungsbereich in Indien auf. Anschließend übernahm er als Managing Director die Leitung des 100% Bosch-Tochterunternehmens ETAS Automotive India Prv. Ltd.
Von 2015 bis 2018 war Herr Zerfowski im Corporate Sector Automotive System Integration für die strategische Ausrichtung der Software-Themen im Automotive-Bereich der Firma Bosch verantwortlich. Seit Mai 2018 ist er in der Bosch-Tochter ETAS im Bereich Security und Vehicle Run Time Environment zuständig.

Kontakt

Email: Detlef.Zerfowski@etas.com