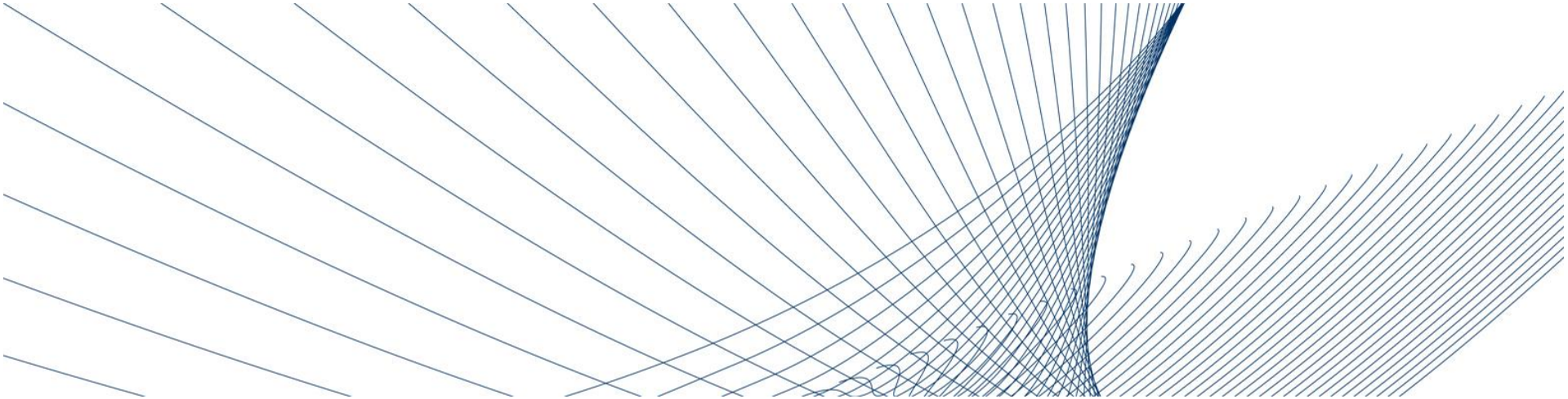
VOLKSWAGEN

AKTIENGESELLSCHAFT



Einfluss der Security-Prämissen auf die Fahrzeugarchitektur

6. IT-Forensik Workshop an der FH Aachen am 18. Mai 2016

Vortragende: Anna-Katharina Gerstel

Stand: 26.04.2016 Abteilung: EEIN-4

Inhaltsverzeichnis

Angriffspunkte moderner Fahrzeuge

eCall, Car-Net, Mobile Online-Dienste

Mobiltelefon, etc.

Mobilfunk
(UMTS, GPRS, LTE, etc.)

Mobiltelefon, etc.

NFC

Ampel, etc.

Car to X

Sondereinsatz-Fzg.

Car to Car

Laptop, iPad etc.

Bluetooth

WLAN

Reifendruck-kontrolle

PLC

Ladesäule

Datenträger
CD, DVD,SD-Card, etc.

Mediadaten
MP3, JPEG, MPEG

Diagnose
OBD, DoIP

Konstruktion
Geschützter Einbauort etc.

Software-Funktionen
Komponentenschutz, Wegfahrsperre etc.

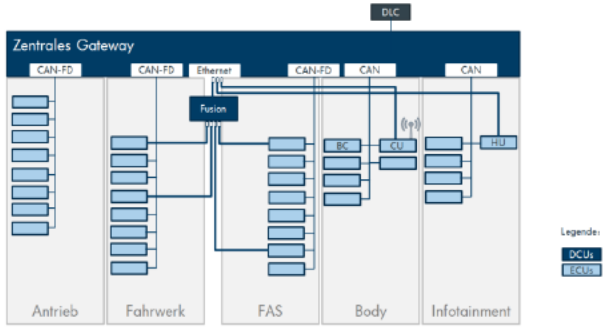
Funkschlüssel
z.B. Keyless Go

Aufgaben der Fahrzeugarchitektur

Eingangsparameter

- Antrieb
- Fahrwerk
- Komfort
- FAS/IS
- Infotainment
- …

E/E-Architektur



Kriterien

E/E Architektur – Festlegung Vernetzungskonzept inkl. Steuergerätetopologie auf Basis von Funktionsanforderungen und technischen Kriterien

Vernetzungsbild in Anlehnung an V. Navale, K. Lagospiris, A. Schaffert, et al.: „(R)evolution of E/E-Architectures", in SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 8 (2), Seite 282-288, unter: http://papers.sae.org/2015-01-0196/e (abgerufen am 25.04.2016)

Architekturprämissen Security

Anwendungsregeln für die Verortung von Funktionen und Steuergeräten:

1. Außenschnittstellen minimieren & konzentrieren

- Drahtlose & drahtgebundene Datenschnittstellen außerhalb des Fahrzeug-internen Netzwerks *auf wenige Komponenten im Fahrzeug beschränken*

2. Fahrzeug-interne Vernetzung segmentieren

- Einführung von *Security-Zonen* um Funktionen unterschiedlicher Kritikalität voneinander zu entkoppeln

3. Kommunikation kontrollieren

- Datenkommunikation an Außenschnittstellen und zwischen Security-Zonen kontrollieren bzw. nur nötige Daten routen

Zielsetzung der Arbeit

Was bedeutet Security by design im Aufgabenfeld des Fahrzeugarchitekten?

- Wie wird Security bisher in die Architekturentwicklung integriert?
- Welche Möglichkeiten unter dem Gesichtspunkt „Digitalisierung“ hat die Architektur um Security bei bestehenden Fahrzeugkonzepten umzusetzen?
- Welche Möglichkeiten hat die Architektur in Zukunft, wenn sie völlig neue Entwicklungsansätze verwenden kann?

Ziel der Arbeit→ Erstellung von Anwendungsregeln bzw. einer Vorgehensmethodik für die Architekturauslegung

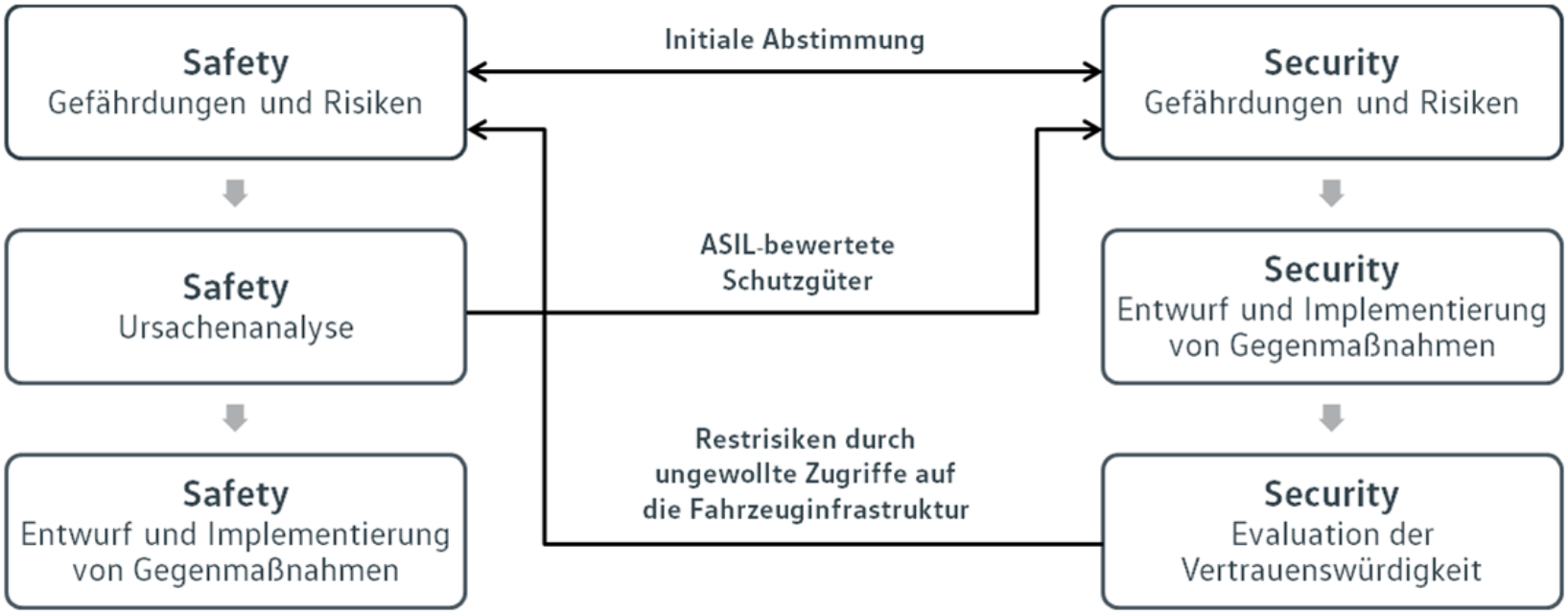
Zielsetzung der Arbeit

Was bedeutet Security by design im Aufgabenfeld des Fahrzeugarchitekten?

- Wie wird Security bisher in die Architekturentwicklung integriert?
- Welche Möglichkeiten unter dem Gesichtspunkt „Digitalisierung“ hat die Architektur um Security bei bestehenden Fahrzeugkonzepten umzusetzen?
- Welche Möglichkeiten hat die Architektur in Zukunft, wenn sie völlig neue Entwicklungsansätze verwenden kann?

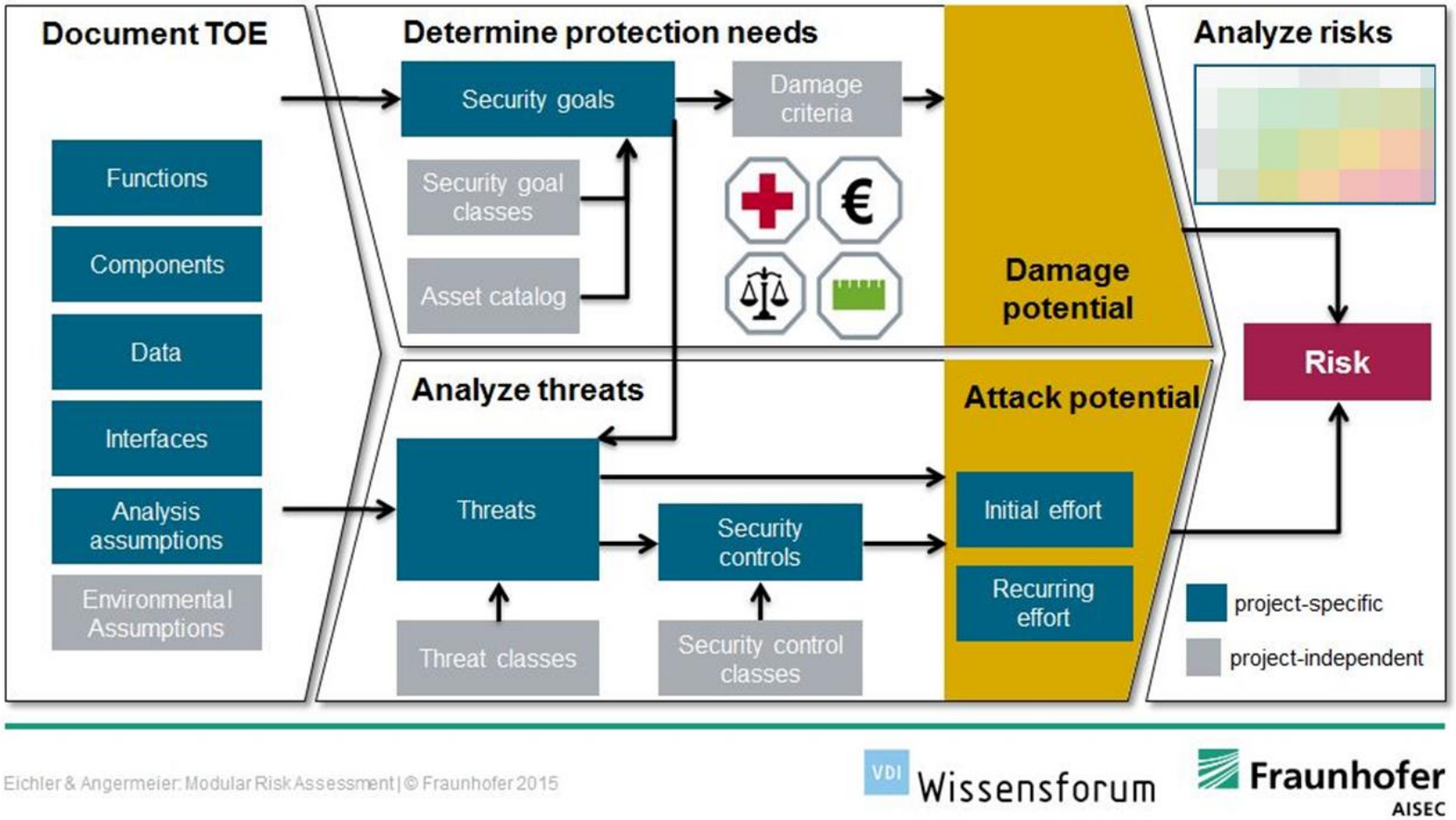
Ziel der Arbeit→ Erstellung von Anwendungsregeln bzw. einer Vorgehensmethodik für die Architekturauslegung

Bisherige Abstimmung zwischen Safety und Security



Dr. C. Robinson-Mallett, Dr. B. Kaiser, J. Müller: „Sicherheit für vernetzte Fahrzeuge“, in ATZ (10/2014), unter:
http://www.berner-mattner.com/cms/upload/1_PDF/1_Ueber_uns/Publikationen/BernerMattner_Publikationen_FA_Sicherheit_vernetzte_Fahrzeuge_ATZ_10_2014_DE.pdf (abgerufen am 25.04.2016)

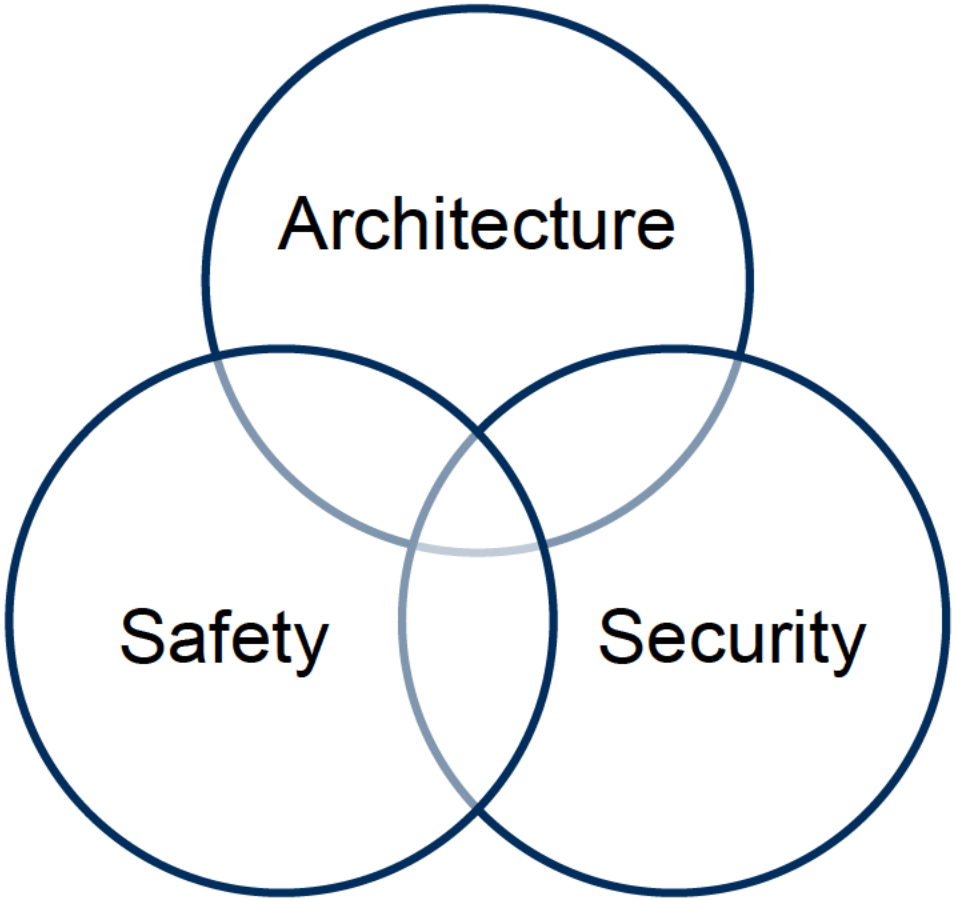
Bisheriges Vorgehen in der Security (Beispiel: Risikoanalyse)



J. Eichler und D. Angermeier, „Modular Risk Assessment for the Development of Secure Automotive Systems," 31. VDI/VW-Gemeinschaftstagung Automotive Security VDI, Wolfsburg, 2015.

Anwendungsregel: Architekturlevel in Anlehnung an *Automotive Safety Integrity Level (ASIL)*[1] und die *Security Level (SecL)*[2]

- Function Impact (FI)
  Worst Case Funktionsauswirkung
- Degree of cross-linking (DCL)
  Vernetzungsgrad der Funktion
- Assault Probability (AP)
  Massenangriffstauglichkeit



1. *ASIL siehe ISO 26262-1:2011(E), "Road vehicles – Functional Safety".*
2. *SecL siehe G. Macher, A. Höller, H. Sporer et al.: „A Combined Safety-Hazards and Security-Theat Analysis Method for Automotive Systems", in „Computer Safety, Reliability and Security – SAFECOMP 2015 Workshops" (09/2015), unter: http://rd.springer.com/chapter/10.1007%2F978-3-319-24249-1_21 (abgerufen am 25.04.2016)*

Resultierende Methoden für die Architekturentwicklung

1. Funktionsverteilung und –mapping
2. [redacted]
3. [redacted]
4. Steuergeräte-oder Funktionsverlagerung (Bustechnologie oder Security-Zonen)
5. [redacted]
6. [redacted]
7. [redacted]
8. [redacted]
9. Netzwerkmanagement (z.B. Cluster Wake-Up)
10. [redacted]
11. [redacted]
12. [redacted]

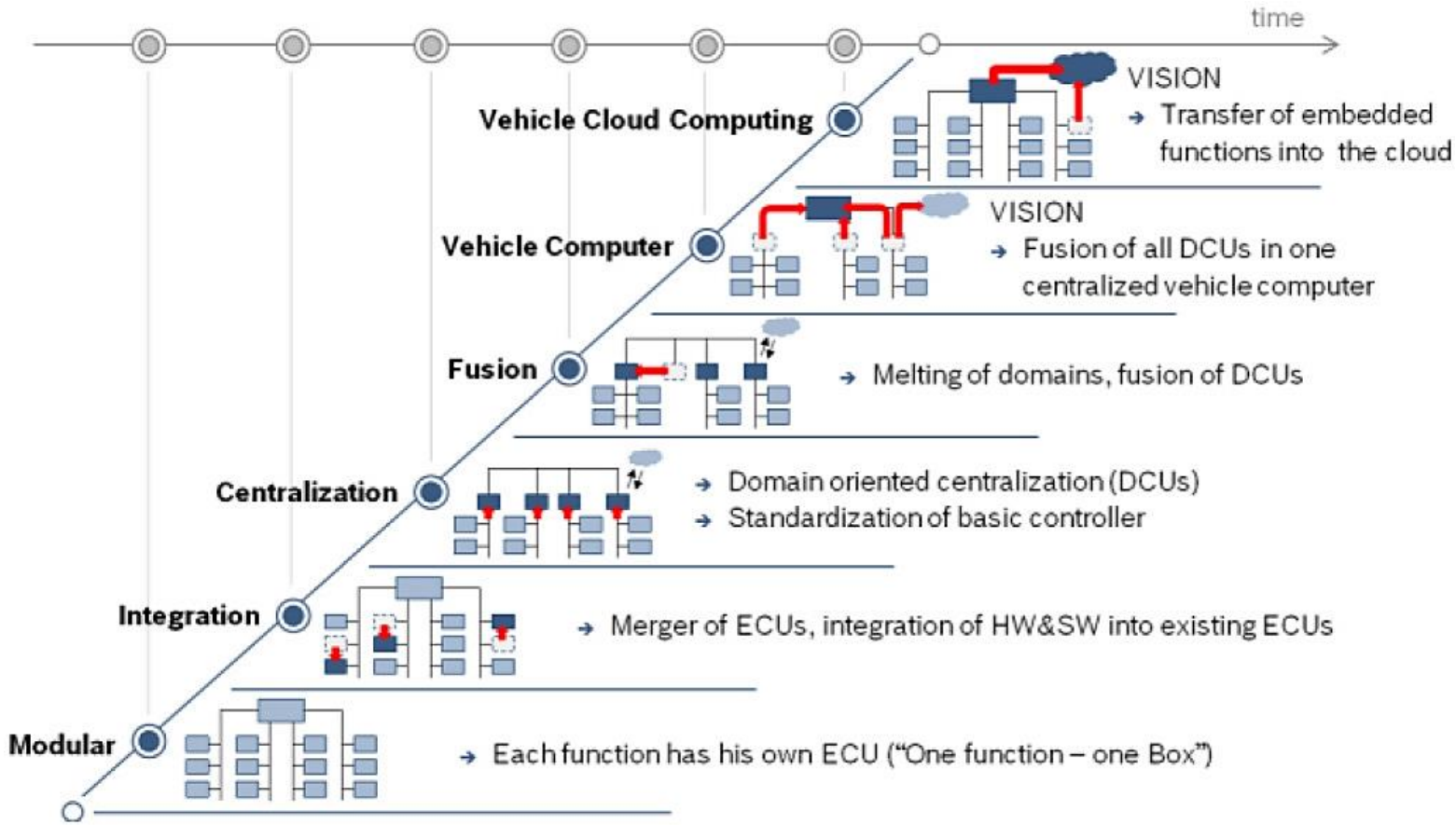
Zielsetzung der Arbeit

Was bedeutet Security by design im Aufgabenfeld des Fahrzeugarchitekten?

- Wie wird Security bisher in die Architekturentwicklung integriert?
- Welche Möglichkeiten unter dem Gesichtspunkt „Digitalisierung“ hat die Architektur um Security bei bestehenden Fahrzeugkonzepten umzusetzen?
- Welche Möglichkeiten hat die Architektur in Zukunft, wenn sie völlig neue Entwicklungsansätze verwenden kann?

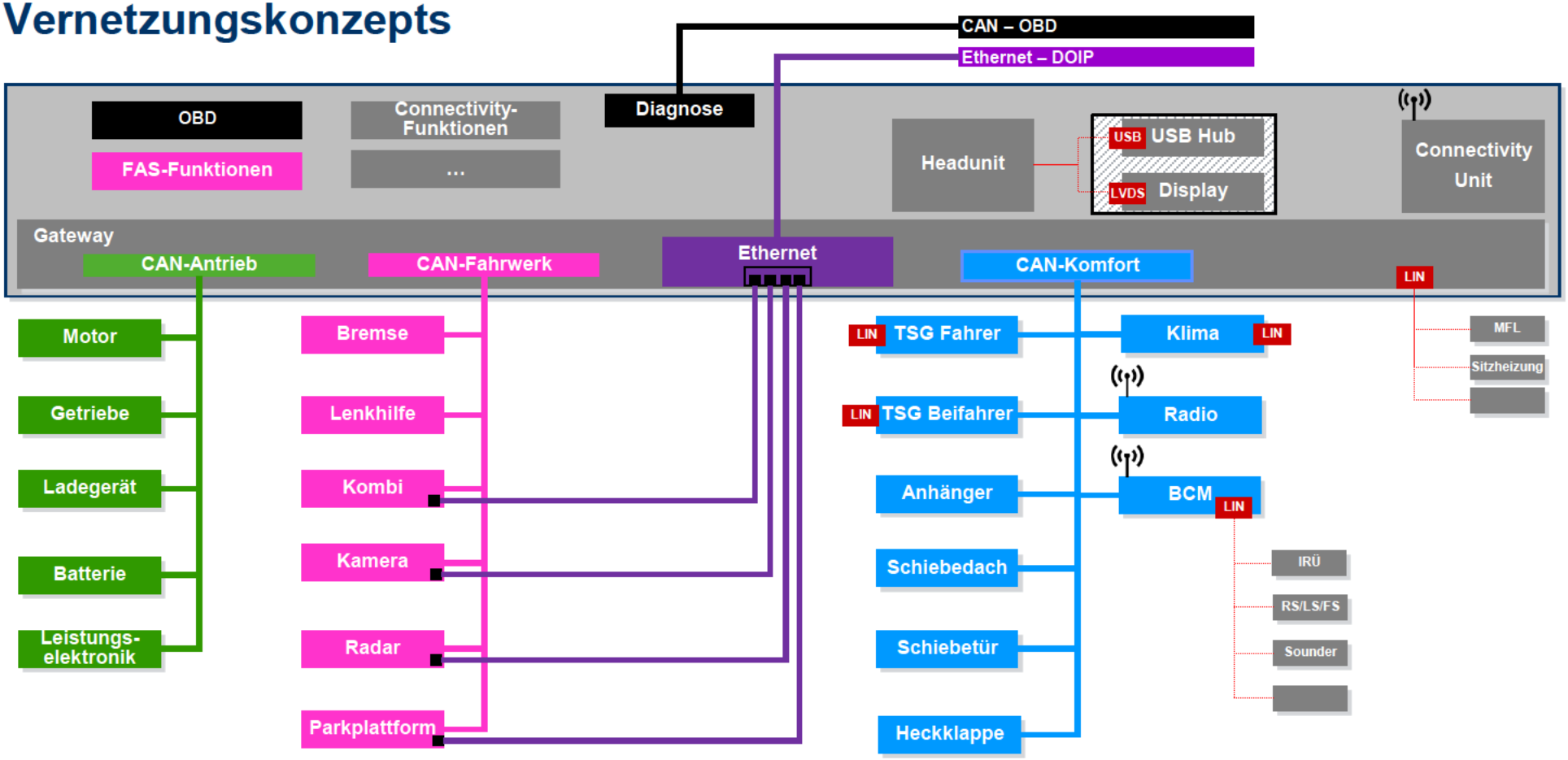
Ziel der Arbeit→ Erstellung von Anwendungsregeln bzw. einer Vorgehensmethodik für die Architekturauslegung

Entwicklung der Fahrzeugarchitektur



V. Navale, K. Lagospiris, A. Schaffert, et al.: „(R)evolution of E/E-Architectures", in SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 8 (2), Seite 282-288, 04/2015, unter: http://papers.sae.org/2015-01-0196/ (abgerufen am 25.04.2016)

Entwicklung der Fahrzeugarchitektur anhand eines exemplarischen Vernetzungskonzepts



Resultierende Prämissen zur Absicherung moderner Architekturen

1. Externe Schnittstellen reduzieren und minimieren
2. [redacted]
3. Schnittstellen (insbesondere für externe Kommunikation) abstrahieren
4. [redacted]
5. [redacted]
6. [redacted]
7. Intrusion Detection und Logging von Anomalien
8. [redacted]
9. Sicheres Einbringen von Schlüsseln
10. [redacted]
11. [redacted]
12. [redacted]

VOLKSWAGEN

AKTIENGESELLSCHAFT

Haben Sie noch Fragen?

VOLKSWAGEN

AKTIENGESELLSCHAFT

Vielen Dank für Ihre Aufmerksamkeit!