

# Anwendungen 1:

## Informationssicherheit in Fahrzeugnetzen

Philipp Meyer

Hamburg University of Applied Sciences  
philipp.meyer@haw-hamburg.de



Hochschule für Angewandte  
Wissenschaften Hamburg  
*Hamburg University of Applied Sciences*



SPONSORED BY THE

Federal Ministry  
of Education  
and Research

## Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

**1** Arbeitsgruppe

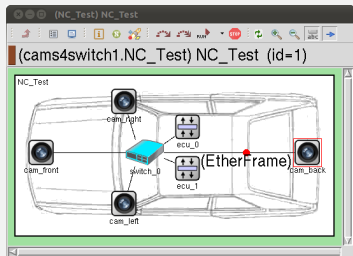
**2** Einleitung & Motivation

**3** Schutzbedarf

**4** Schutzkonzepte

**5** Zusammenfassung & Ausblick

- 15+ Studenten
- Themenschwerpunkt: Echtzeit Ethernetprotokolle für Fahrzeugnetze
- Umsetzungen in Simulationen und Prototypen



Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

Anwendungen 1

Philipp Meyer

Arbeitsgruppe

**Einleitung &  
Motivation**

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

**1** Arbeitsgruppe

**2** Einleitung & Motivation

**3** Schutzbedarf

**4** Schutzkonzepte

**5** Zusammenfassung & Ausblick

- Vielzahl an Sensoren und Steuergeräten(ECUs)
- Von proprietären Bustechnologien zu Ethernet
- Gegenwärtige Infrastrukturen sind angreifbar
- Informationssicherheit wichtiges Ziel für die nächste Bordnetzgeneration

### Vorteile:

- Erprobte Technologie
- Geordnete Infrastruktur
- Hohe Bandbreiten
- IP-basierte Dienste

### Nachteil:

- Sicherheitsrisiken durch Verbreitung

Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

**1** Arbeitsgruppe

**2** Einleitung & Motivation

**3** Schutzbedarf

**4** Schutzkonzepte

**5** Zusammenfassung & Ausblick

Funktionssicherheit („safety“):

- Spezifizierte Funktionalität ist Umgesetzt
- System läuft korrekt und zuverlässig

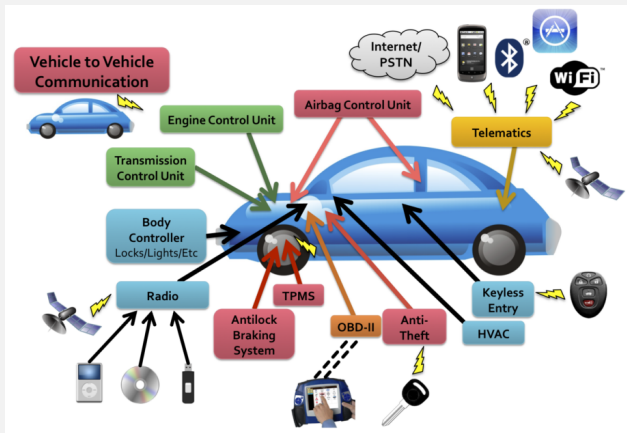
Informationssicherheit („security“):

- Es gibt keine unautorisierten Veränderungen von Informationen
- Geheimhaltung der Informationen

Während die Funktionssicherheit schon im Fokus der Hersteller steht muss nun auch die Informationssicherheit immer mehr ins Visier genommen werden.



- Geheimhaltung (Informationsvertraulichkeit)
- Schutz vor Modifikation (Datenintegrität)
- Schutz vor Performanceverlust (Systemverfügbarkeit)



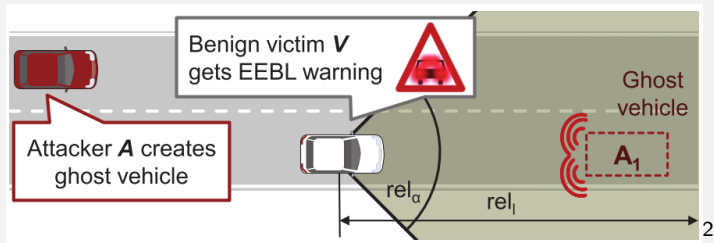
1

<sup>1</sup> Stephen Checkoway u. a. „Comprehensive Experimental Analyses of Automotive Attack Surfaces.“ 2011.

- Vollzugriff auf das Fahrzeugsystem
- Konfiguration über Windows-basierte PCs
- Verbunden mit „PassThru“ Gerät (USB oder WLAN)
- PC hat oft Verbindung zum Internet

Hat der Angreifer die Kontrolle über den PC kann er Fahrzeuge über die Diagnoseschnittstelle Sabotieren!

- Angreifer erzeugt Geisterfahrzeug
- Opfer reagiert auf das scheinbar vorhandene Auto:
  - Warnung!?
  - Automatischer Bremsvorgang!?



<sup>2</sup> N. Bissmeyer u. a., „Short paper: Experimental analysis of misbehavior detection and prevention in VANETs“. 2013.

- Chiptuning
- Tachomanipulation
- Diebstahl (Keyless-Entry)
- Ausspähen des Fahrverhaltens

Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

**Schutzkonzepte**

Zusammenfassung &  
Ausblick

**1** Arbeitsgruppe

**2** Einleitung & Motivation

**3** Schutzbedarf

**4** Schutzkonzepte

**5** Zusammenfassung & Ausblick

## Herausforderungen:

- Harte Echtzeitanforderungen an Teile der Kommunikation
- Begrenzte Rechenleistung der ECUs
- Eingeschränkte Möglichkeit von Softwareupdates
- Verteilte Systemarchitektur
- Lange Produktlebenszyklen
- Vorgaben durch den Gesetzgeber

- PRESERVE<sup>3</sup> (Fokus: V2V und V2X Kommunikation)
- EVITA<sup>4</sup> und SEIS<sup>5</sup> (Fokus: Bordnetze)

<sup>3</sup> **PRESERVE**: *Preparing Secure Vehicle-to-X Communication Systems.*

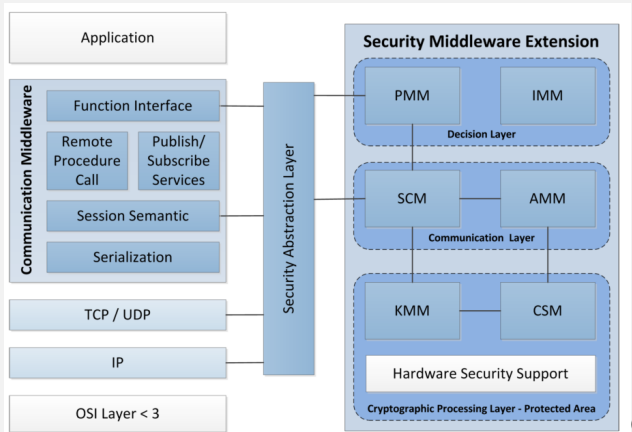
<sup>4</sup> **EVITA**: *E-safety vehicle intrusion protected applications.*

<sup>5</sup> **SEIS**: *Sicherheit in Eingebetteten IP-basierten Systemen.*



## Einsatz von Erprobten Technologien aus der IT-Sicherheit:

- IPsec
- MACsec



6

Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

<sup>6</sup> Alexandre Bouard u. a.: „Driving Automotive Middleware Towards a Secure IP-based Future“. 2012.

- Konzept für ein rein IP-basiertes Netz
- Direkter Hardwarezugriff?

Anwendungen 1

Philipp Meyer

Arbeitsgruppe

Einleitung &  
Motivation

Schutzbedarf

Schutzkonzepte

Zusammenfassung &  
Ausblick

- 1 Arbeitsgruppe
- 2 Einleitung & Motivation
- 3 Schutzbedarf
- 4 Schutzkonzepte
- 5 Zusammenfassung & Ausblick

- Fahrzeuge sind auch Heute schon angreifbar
- Durch die Vernetzung von Steuergeräten und Fahrzeugen durch Ethernet-Technologien steigt das Risiko
- Werkzeugkasten IT-Sicherheit steht zur Verfügung
- Entwicklung von konkreten Konzepten zur Lösung werden Diskutiert

## Fokussierung auf Informationssicherheit der Hardwarebausteine:

- Bedrohungsanalyse
- Gefahr und Eintrittswahrscheinlichkeit bewerten
- Berechnung der Risiken
- Sicherheitslösungen für Angriffe mit hohem Risiko entwickeln



- Website der CoRE - Arbeitsgruppe:  
<http://core.informatik.haw-hamburg.de>

- [1] Stephen Checkoway u. a. „Comprehensive Experimental Analyses of Automotive Attack Surfaces.“ In: *USENIX Security* (2011). URL: [http://static.usenix.org/events/sec11/tech/full\\\_papers/Checkoway.pdf](http://static.usenix.org/events/sec11/tech/full\_papers/Checkoway.pdf).
- [2] N. Bissmeyer u. a. „Short paper: Experimental analysis of misbehavior detection and prevention in VANETs“. In: *Vehicular Networking Conference (VNC), 2013 IEEE*. 2013, S. 198–201. DOI: 10.1109/VNC.2013.6737612.
- [3] PRESERVE. *Preparing Secure Vehicle-to-X Communication Systems*. URL: <http://www.preserve-project.eu> (besucht am 05.05.2014).
- [4] EVITA. *E-safety vehicle intrusion protected applications*. URL: <http://www.evita-project.org> (besucht am 05.05.2014).



- [5] SEIS. *Sicherheit in Eingebetteten IP-basierten Systemen*.  
URL: <http://strategiekreis-elektromobilitaet.de/public/projekte/seis> (besucht am 05. 05. 2014).
- [6] Alexandre Bouard u. a. „Driving Automotive Middleware Towards a Secure IP-based Future“. In: *10th conference for Embedded Security in Cars (Escar'12)*. Berlin, Germany, 2012.  
URL: [https://www.sec.in.tum.de/assets/staff/alexandre/Escar\\_Paper\\_final.pdf](https://www.sec.in.tum.de/assets/staff/alexandre/Escar_Paper_final.pdf).