Challenges in Automotive Security

Security for connected, autonomous Road Vehicles

Prof. Dr. Dominik Schoop

Hochschule Esslingen, Graduate School and Faculty of Information Technology

30 August 2019, Óbudai Egyetem, Budapest

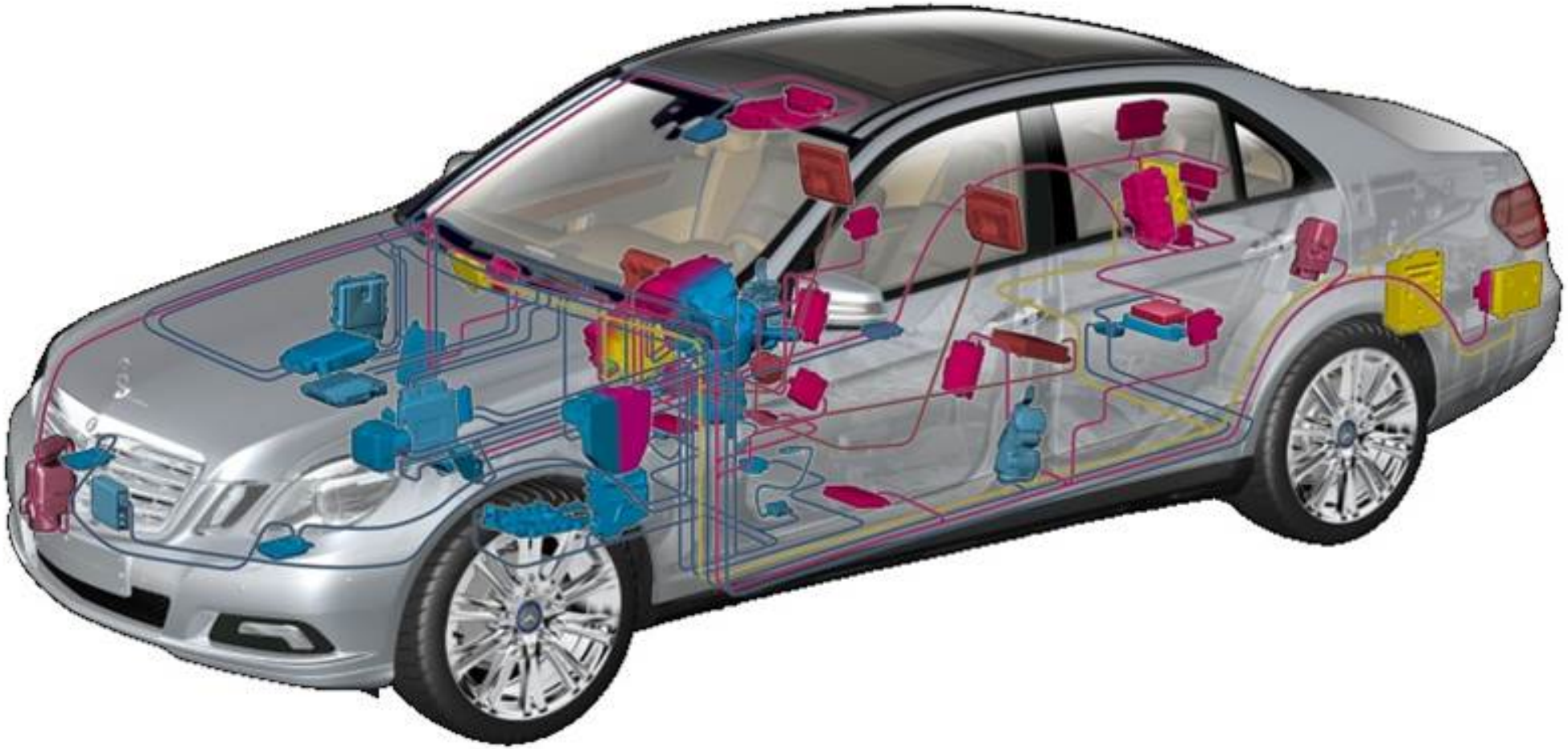
Agenda

1. Attacks on Automotive Systems

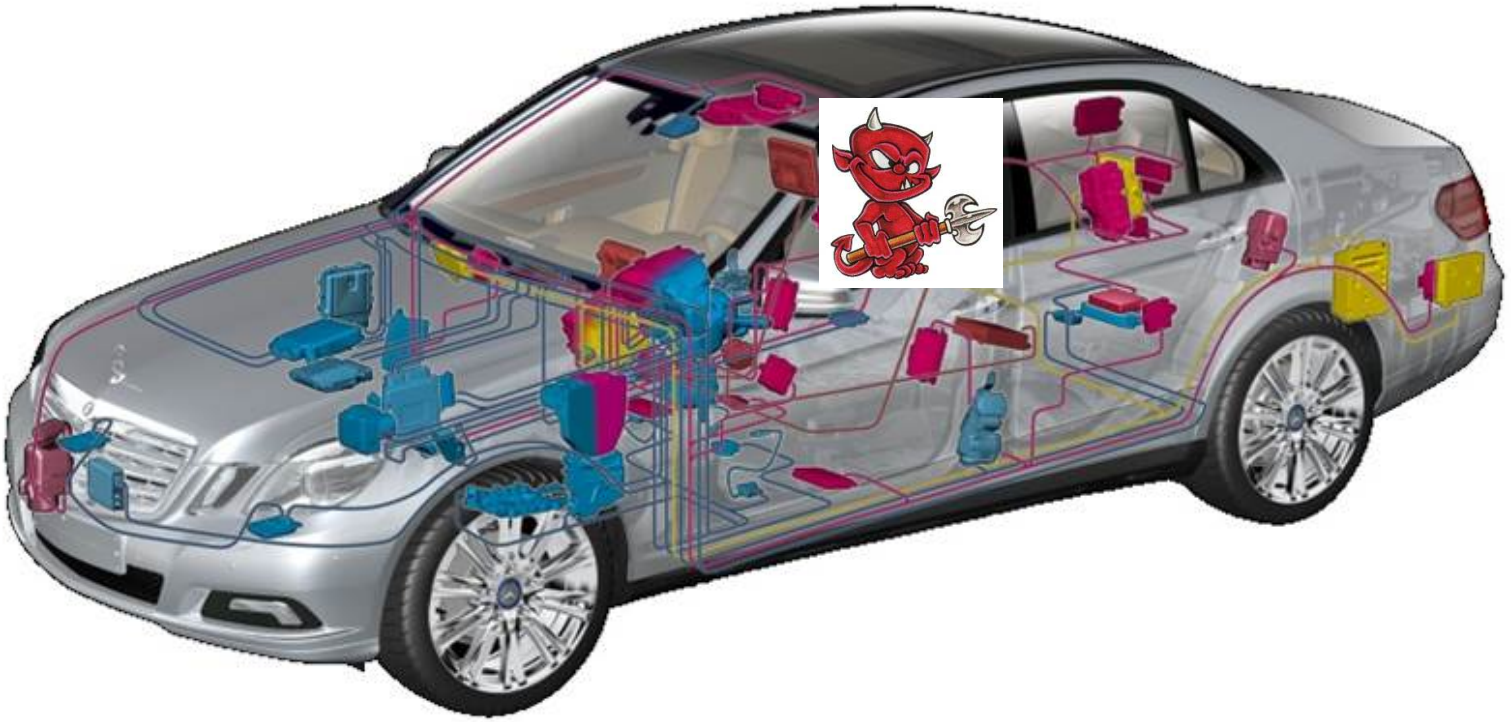
2. Challenges and Solutions

3. Summary

Large number of interconnected components in a vehicle

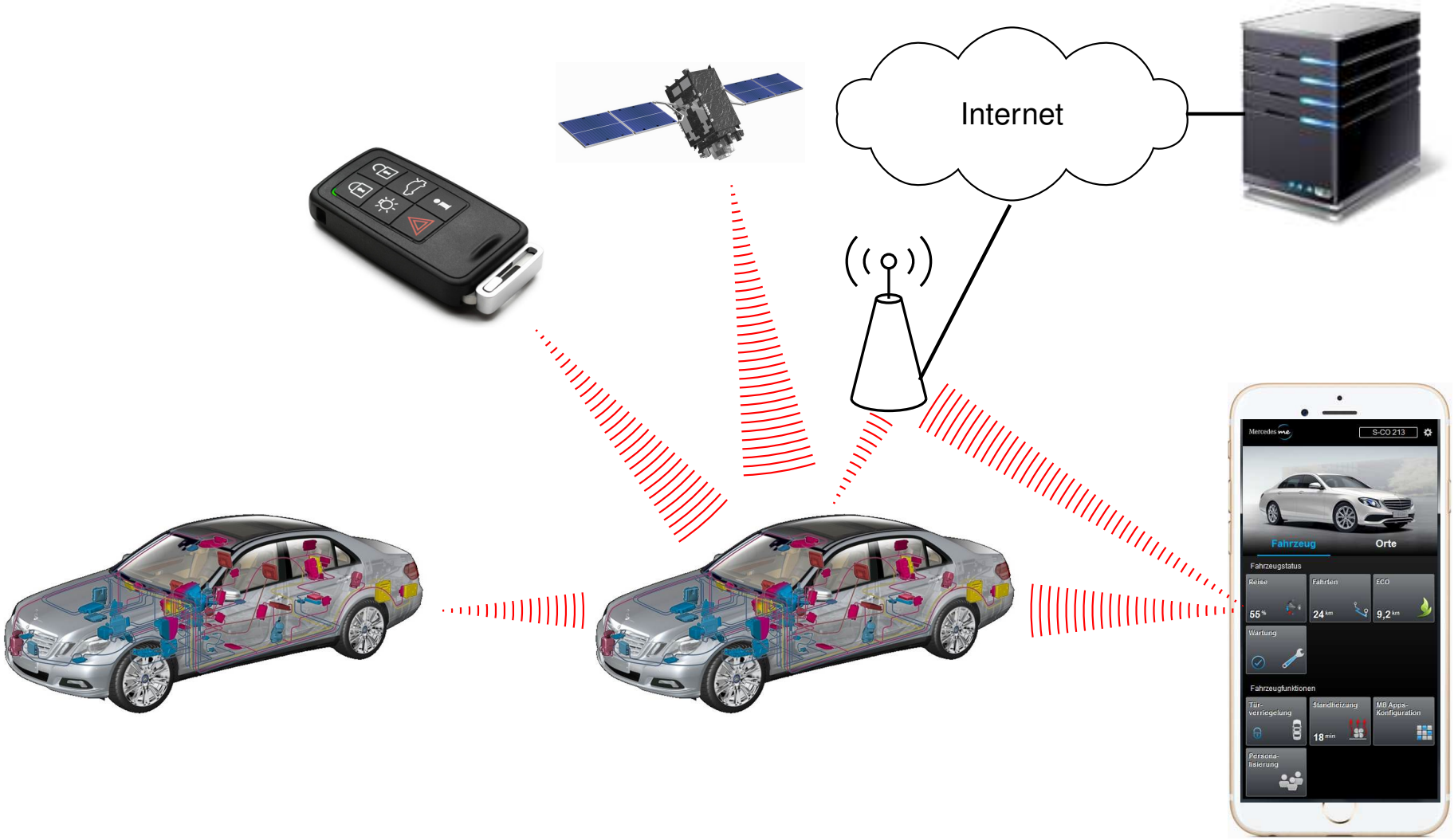


[R. Schmidgall, 2011]

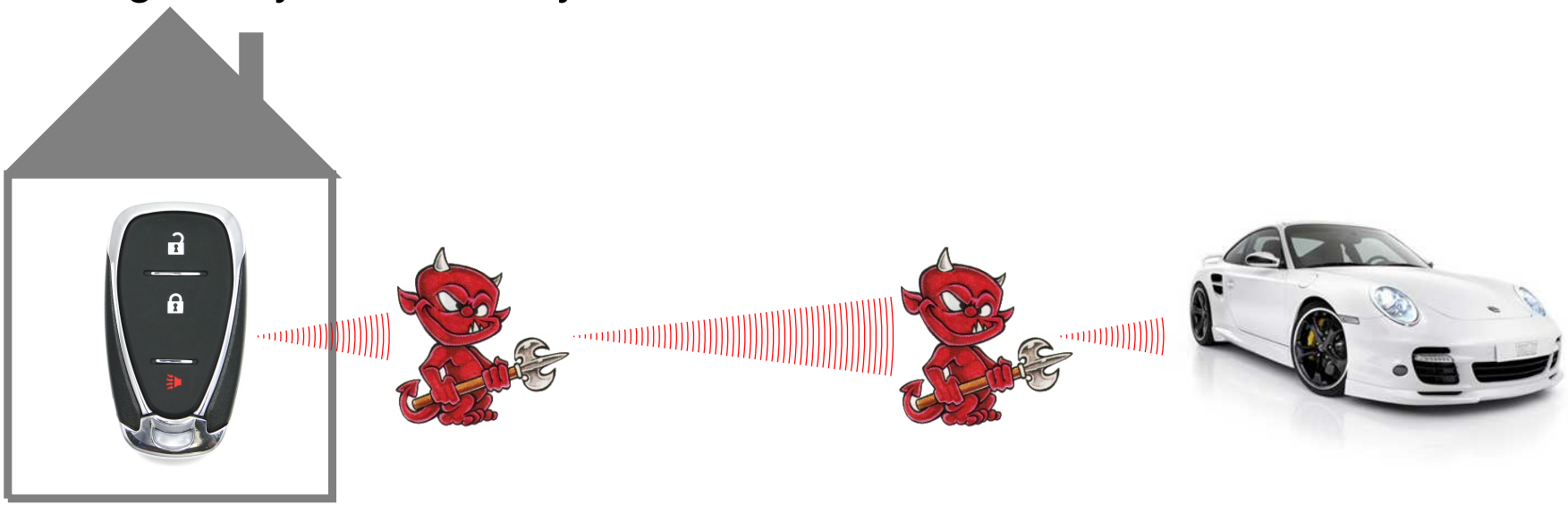


- only limited **authenticity** in automotive bus systems
- system can be manipulated (loss of **integrity**)
- demonstration: Valasek, Miller 2014

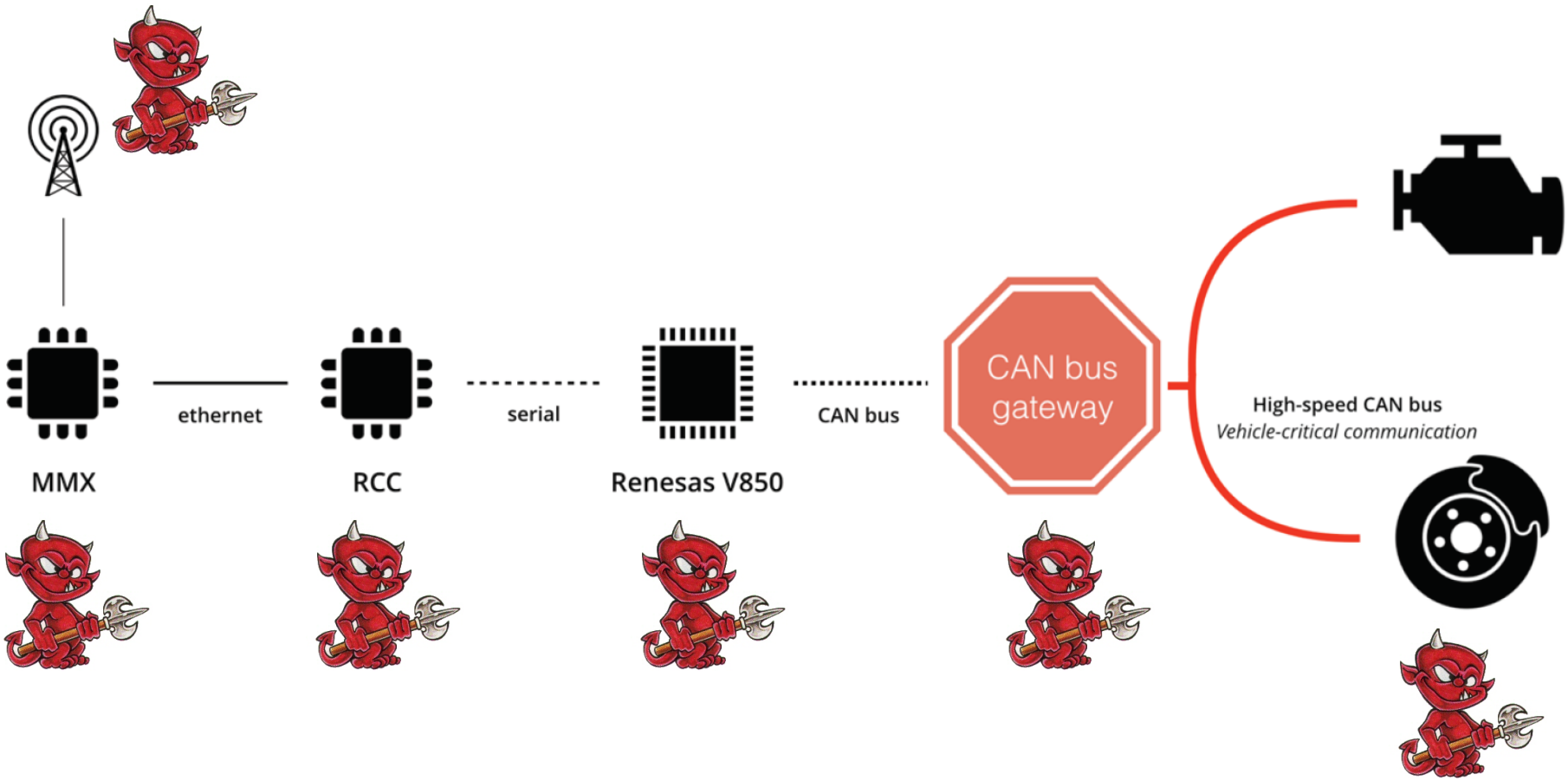
Vehicle as Part of Distributed System



Message relay between key fob and vehicle:



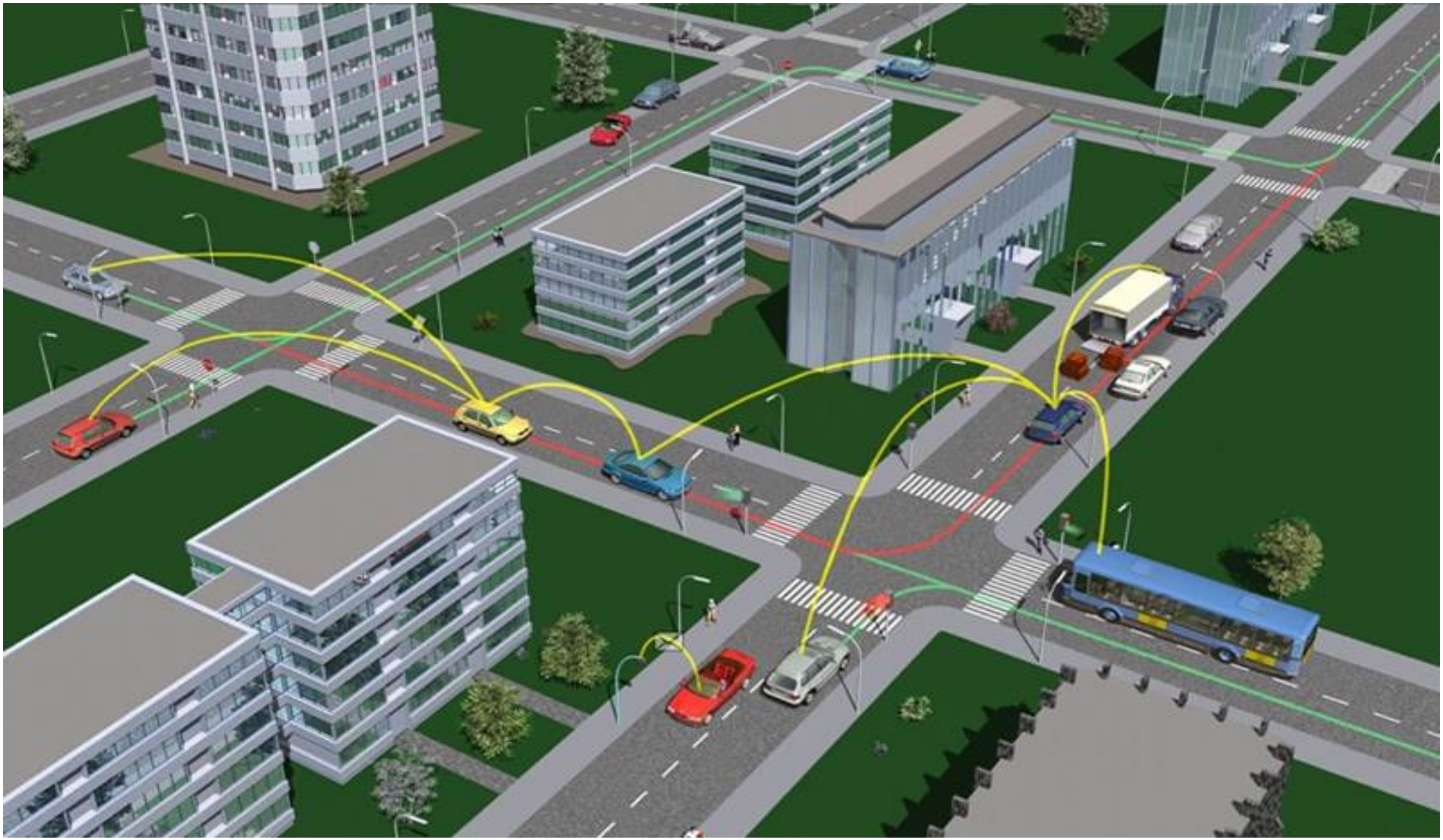
message relay $\rightarrow$ loss of **authenticity of location**



[after The Connected Car, Computest, April 2018]

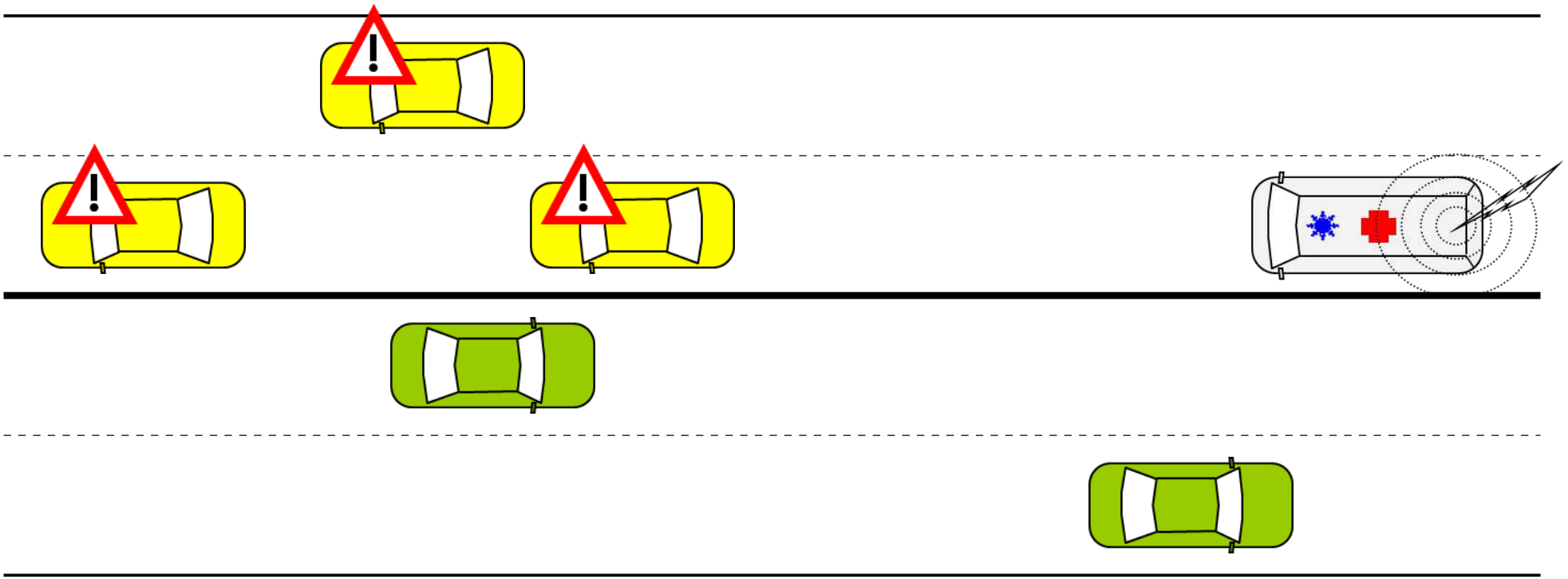
- loss of **authenticity** in communication leads to loss of **integrity**
- demonstrations: Solnik, 2014; Valasek, Miller 2016; Tencent 2019

Communication between vehicle and vehicle or infrastructure (V2X)

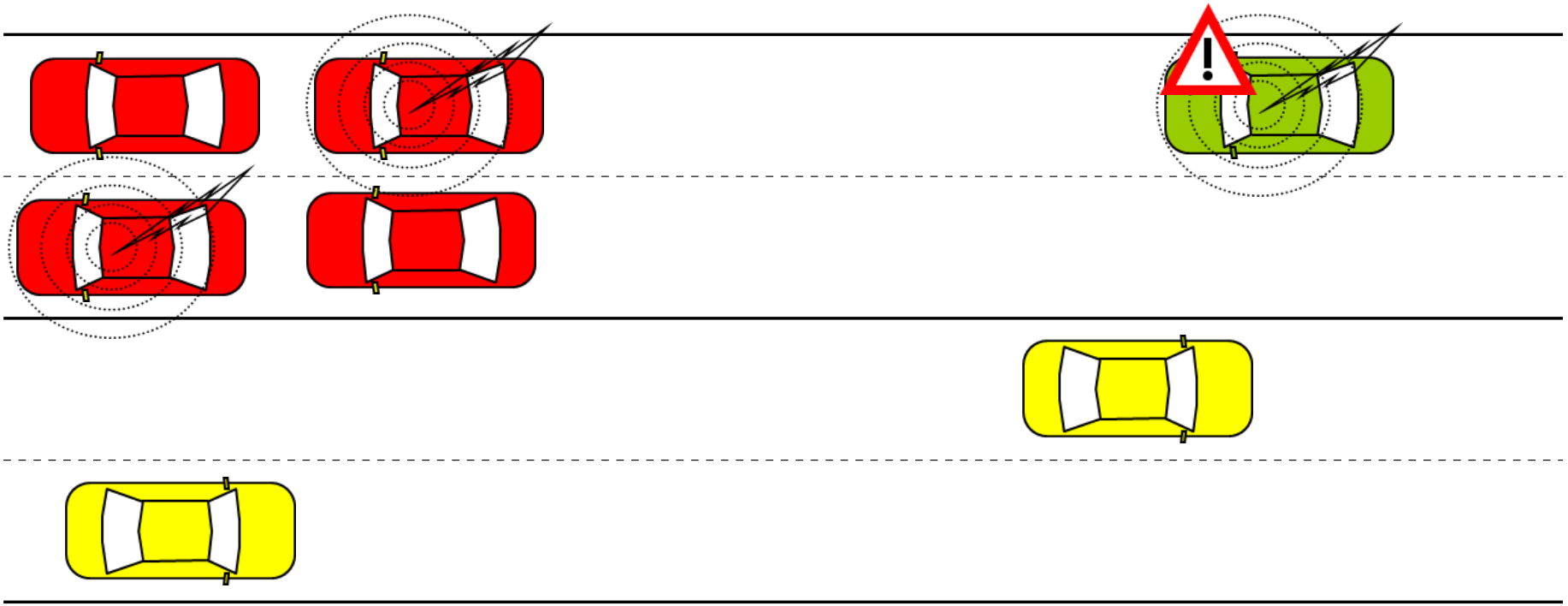


[CAR 2 CAR Communication Consortium, https://www.car-2-car.org/]

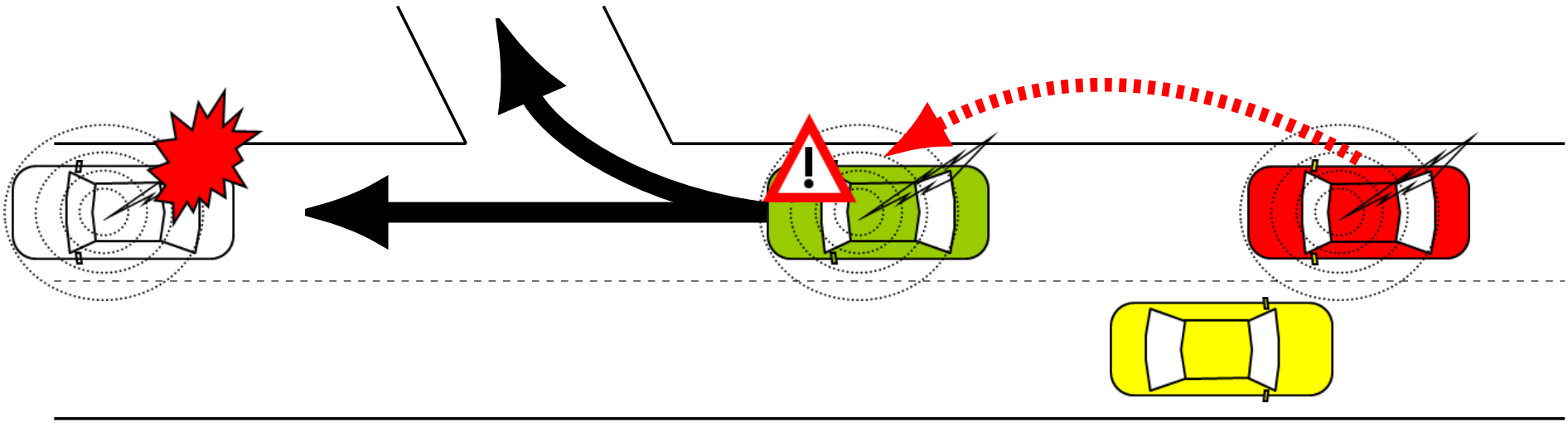
Emergency-vehicle warning



End-of-traffic-jam warning



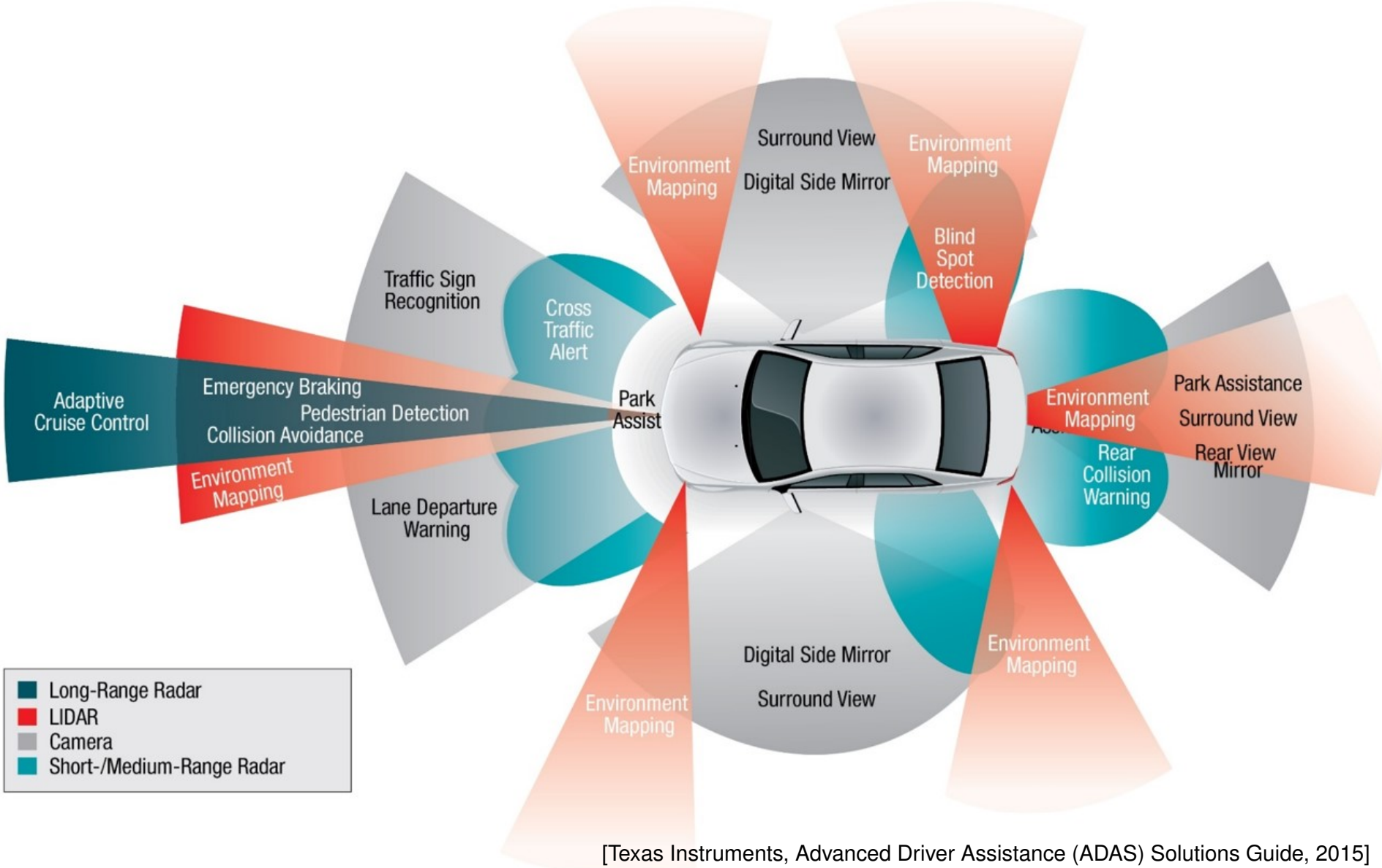
Redirection of vehicles with spoofed messages (missing **authenticity**)



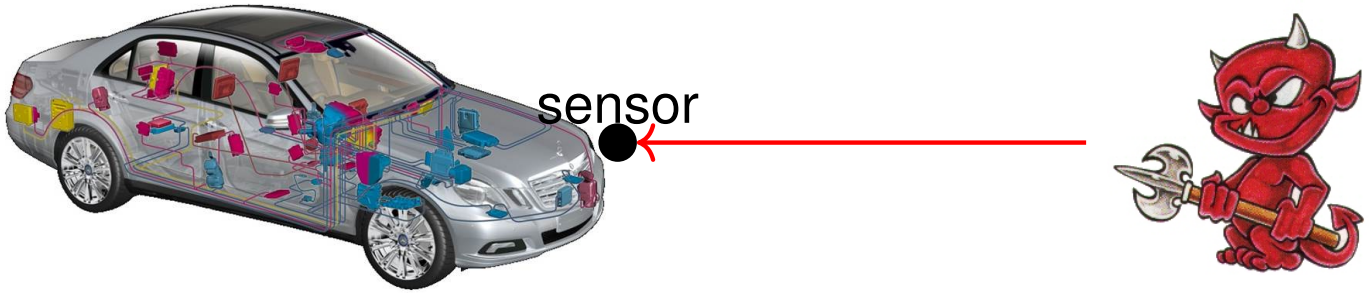
Connected, autonomous Vehicles

Example: Audi A8 Traffic Jam Pilot - SAE Level 3

[Audi AG, AutoBild]



[Texas Instruments, Advanced Driver Assistance (ADAS) Solutions Guide, 2015]



- "Sensor blinding" – render sensor (temporarily) useless by blinding
  Example:
  - laser beam on LIDAR sensor or camera [Petit et al., 2015]
- "Sensor spoofing" – provide faked input for a sensor
  Examples:
  - faked GPS signal [Kexiong et al., 2018]
  - vaseline on rain sensor
  - spoofed LIDAR objects [Petit et al., 2015]
  - spoofed camera images

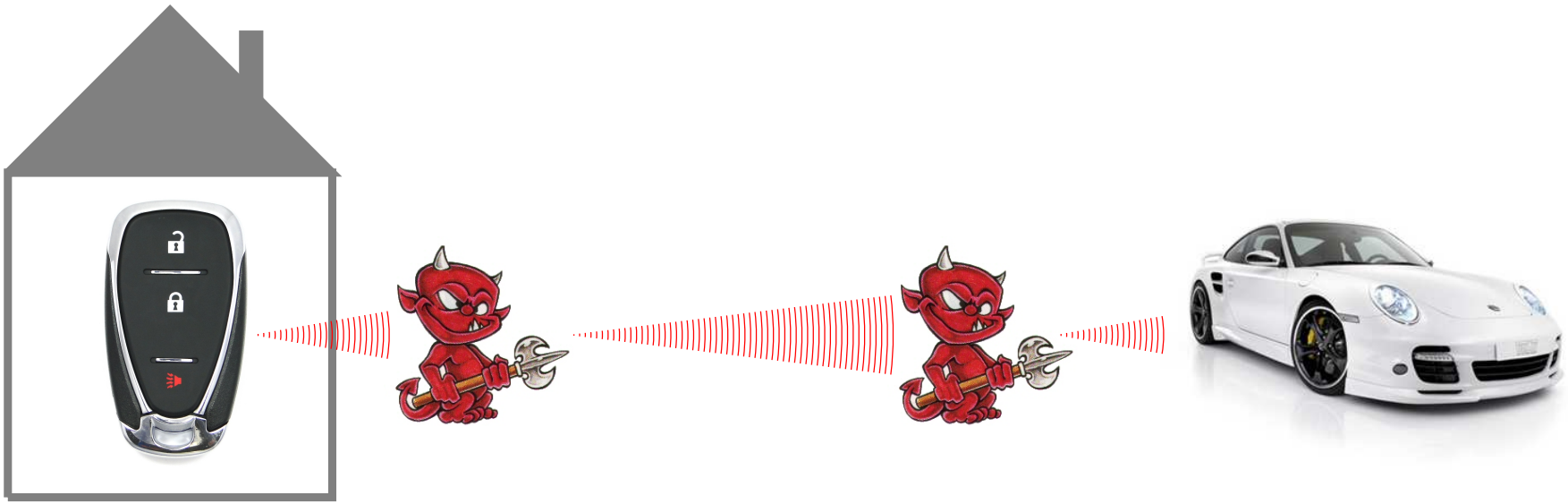
Original sign | Modified sign | Interpretation

[Sitawarin et al., 2018; Eykholt et al., 2018]

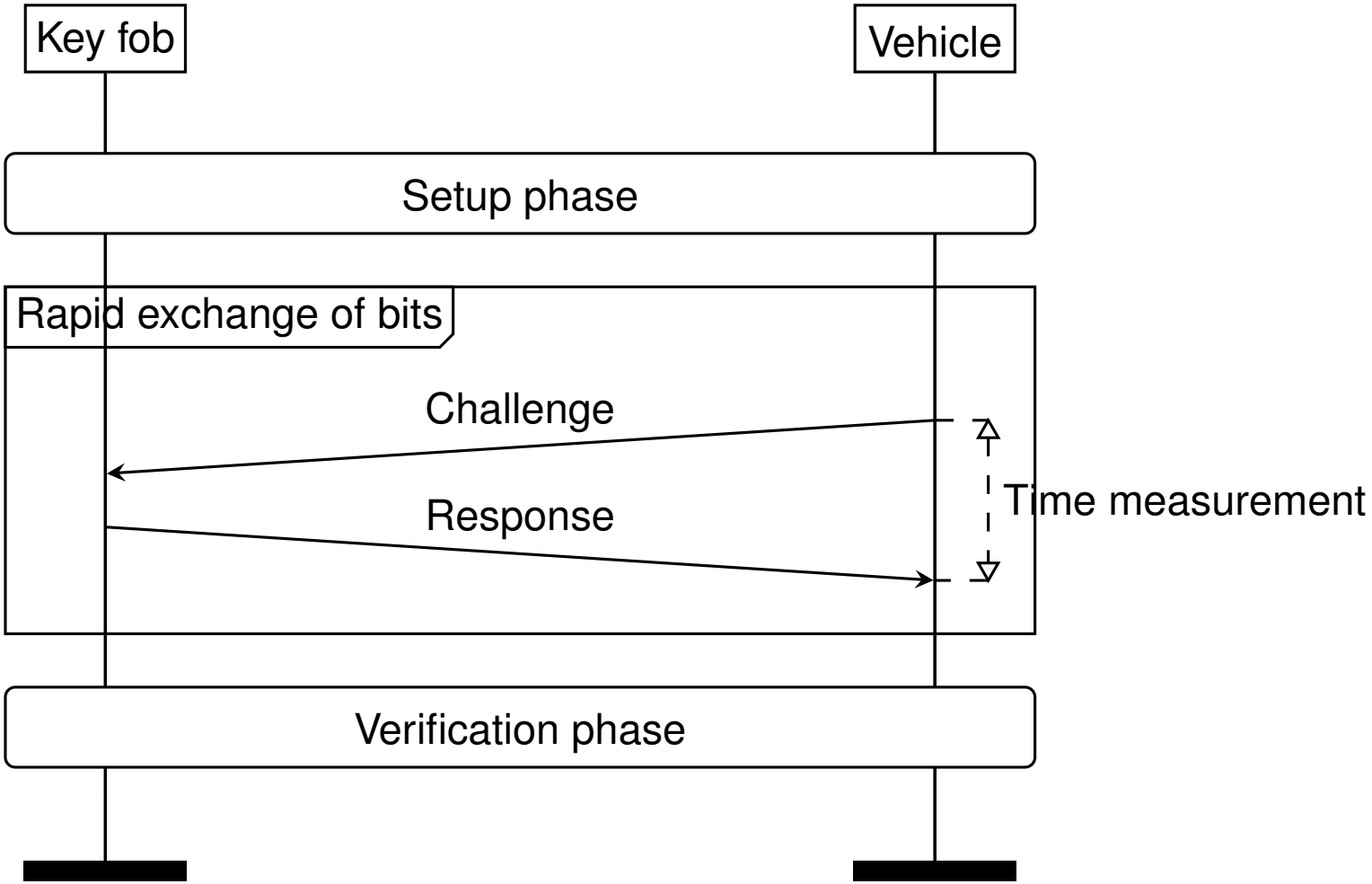
Example: Confusing Tesla Autopilot with dots on the road

[Tencent Keen Security Lab, 2019]

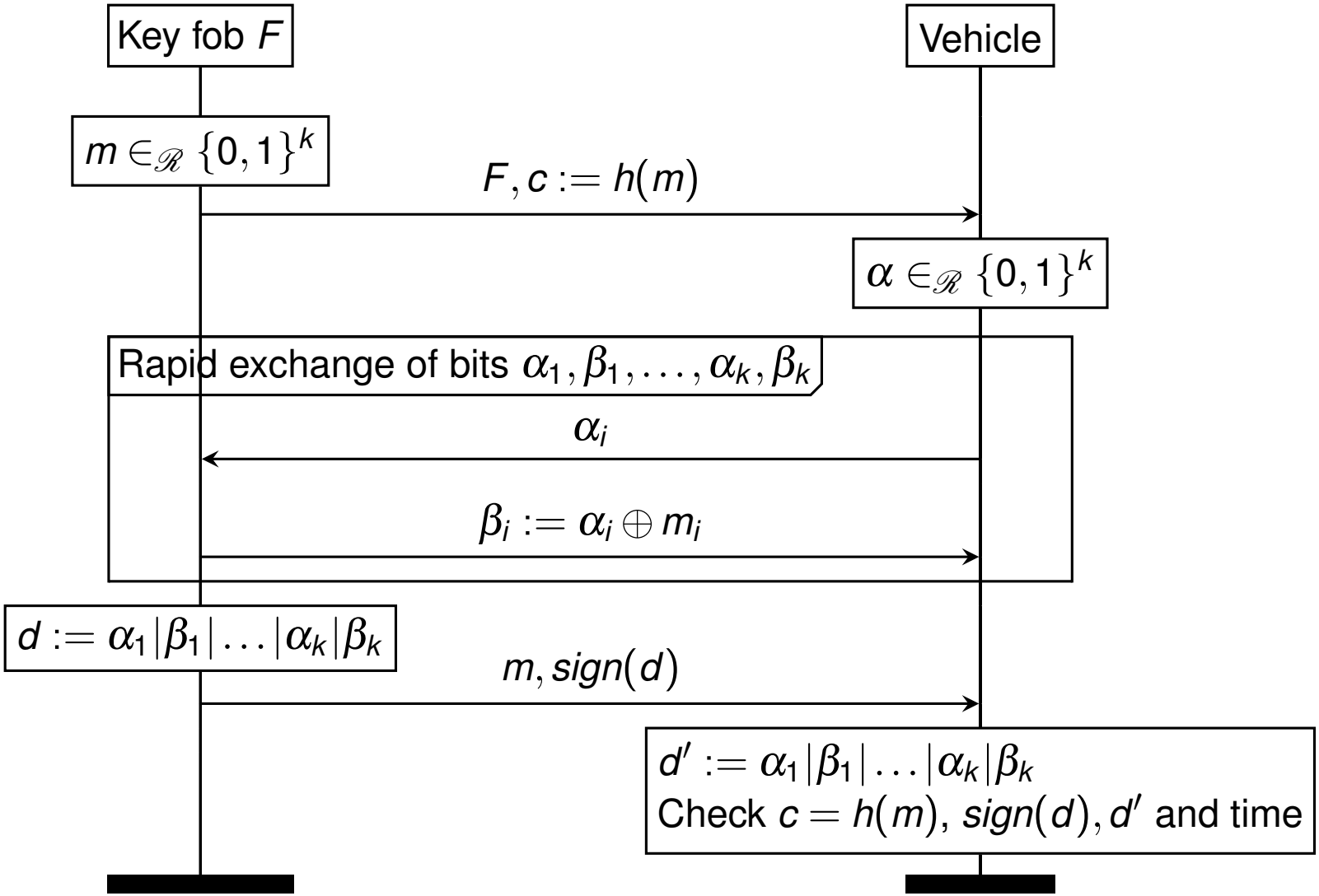
Goal: Vehicle opens if and only if the key fob is close to the vehicle, i.e. messages cannot be relayed (“authenticity of location” of key fob).



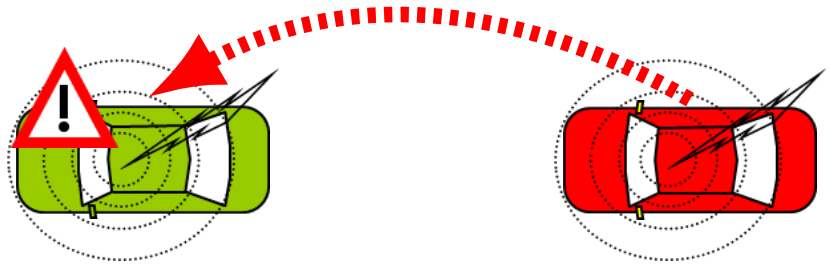
Solution: Distance Bounding Protocol



[after Cremers et al., 2011]



[after Cremers et al., 2011]



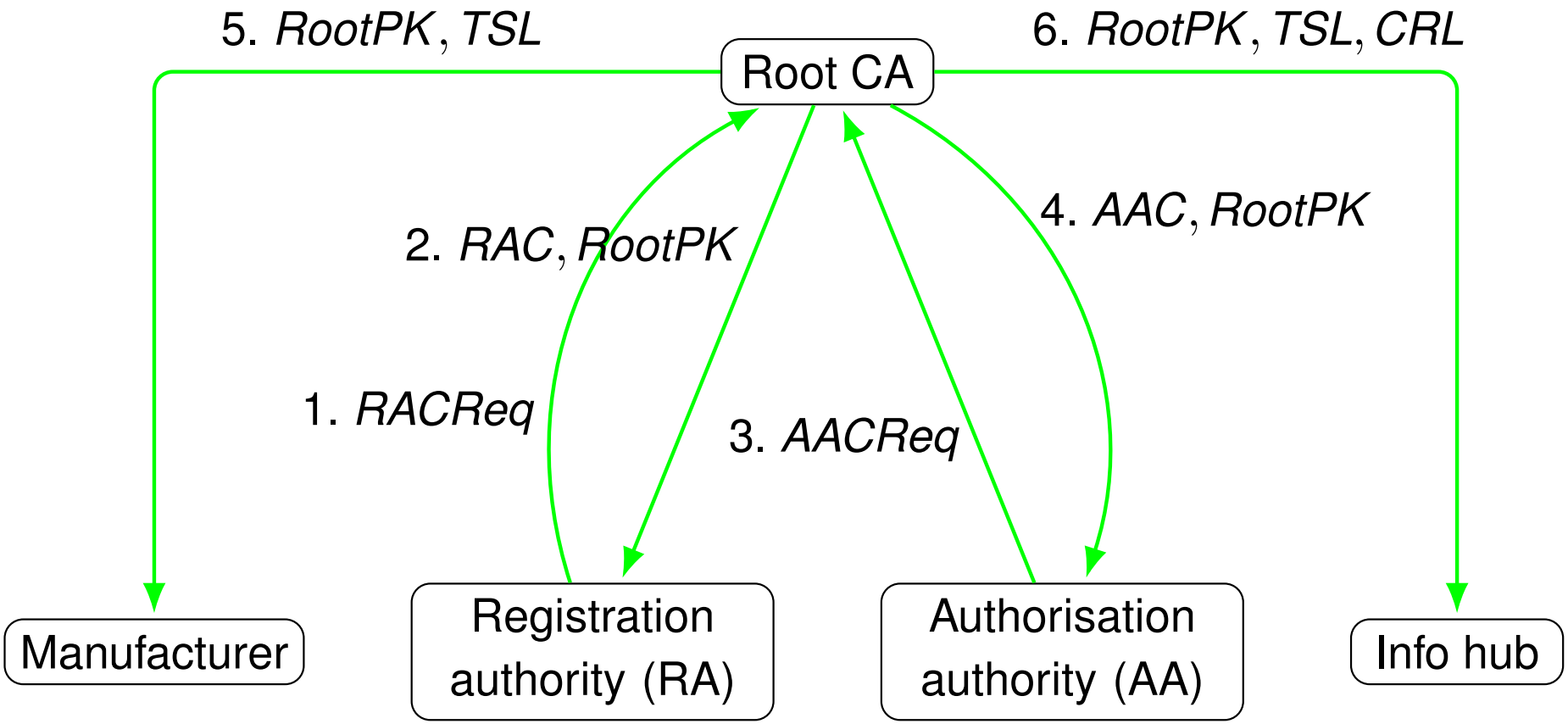
- Authenticity
  - Each message is digitally signed (certificates)
  - Challenge: throughput
- Anonymity
  - Misuse shall be detected
    $\Rightarrow$ no anonymity, only pseudonymity!
- Pseudonymity
  - Pseudonyms are assigned to vehicles by authorities.
  - Pseudonyms have to be changed frequently (unlinkability).
  - Challenge: When to change pseudonyms safely?

authenticity **and** pseudonymity

???

1. Phase: Initialisation of PKI components

$\{m\}_{Sig}$

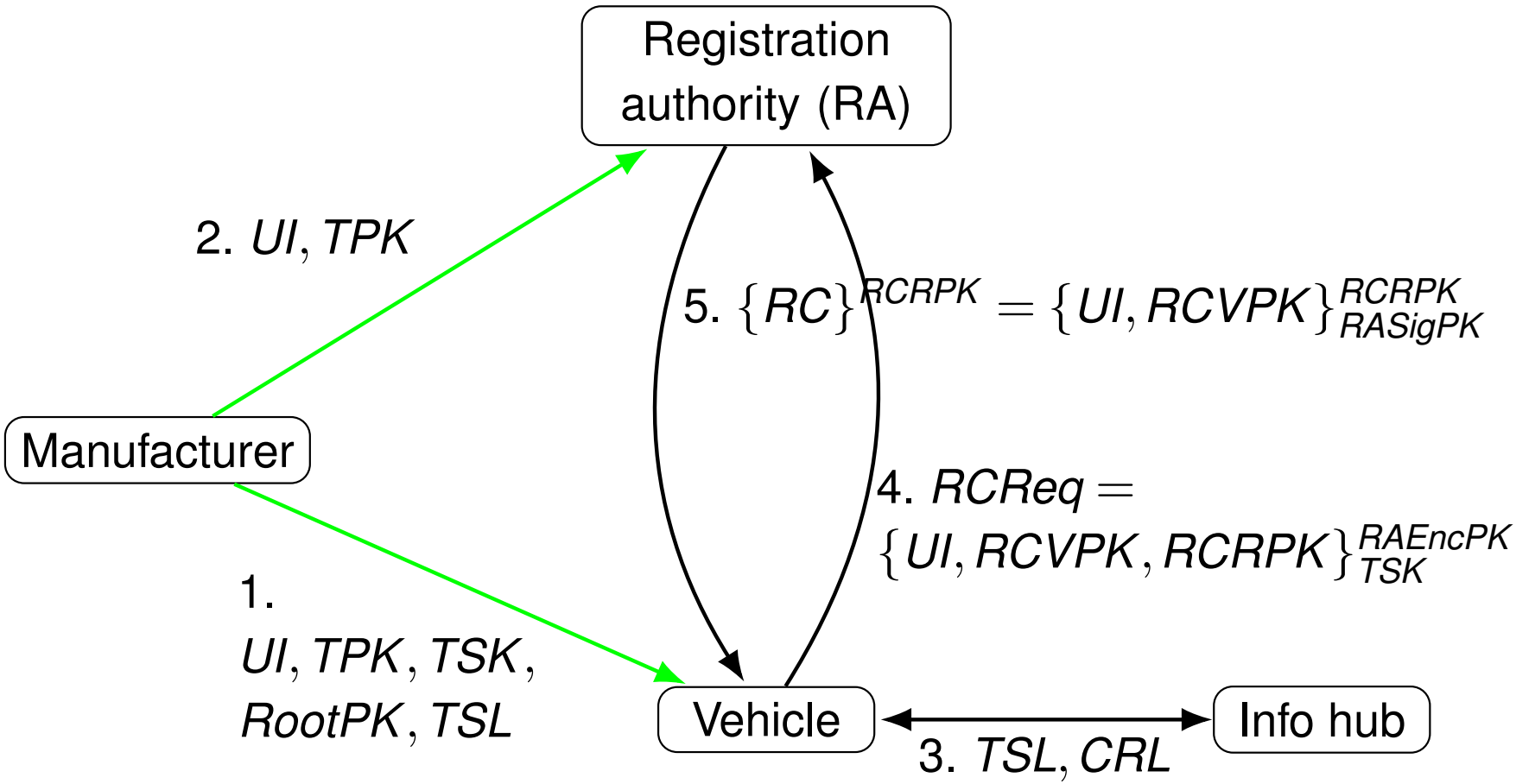


1. $RACReq = \{RA, RASigPK, RAEncPK\}_{RASigPK}$, 2. $RAC = \{RA, RASigPK, RAEncPK\}_{RootSK}$

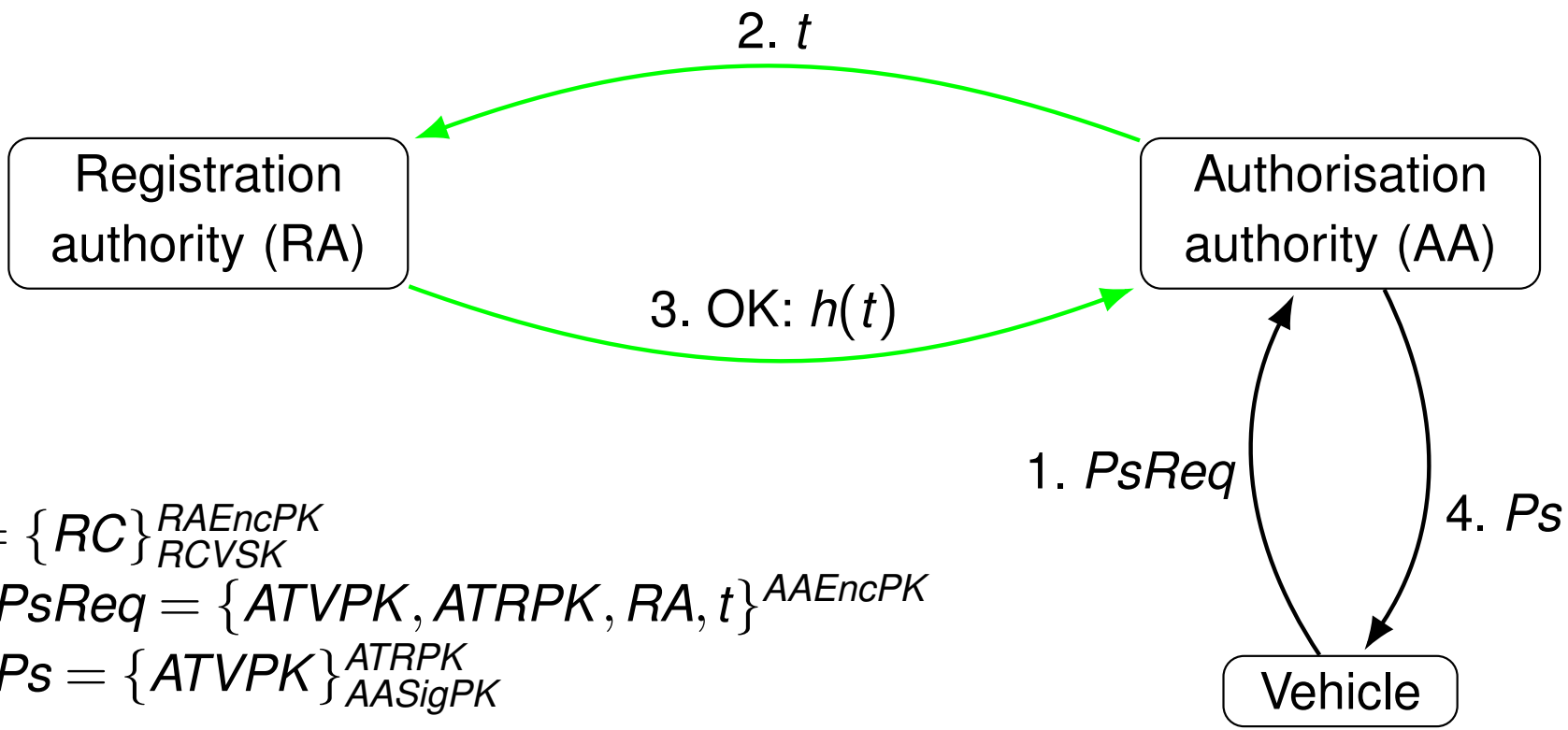
3. $AACReq = \{AA, AASigPK, AAEncPK\}_{AASigPK}$, 4. $AAC = \{AA, AASigPK, AAEncPK\}_{RootSK}$

2. Phase: Registration of vehicle

$\{m\}^{Enc}_{Sig}$



3. Phase: Download of pseudonyms



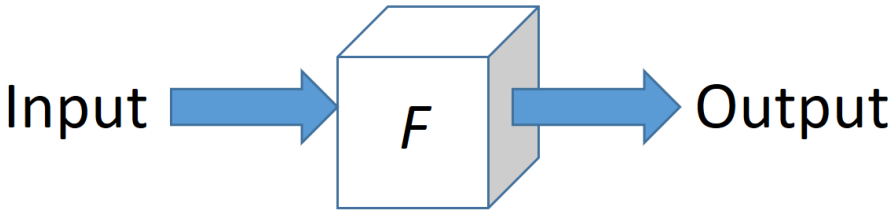
$t = \{RC\}^{RAEncPK}_{RCVSK}$

1. $PsReq = \{ATVPK, ATRPK, RA, t\}^{AAEncPK}$

4. $Ps = \{ATVPK\}^{ATRPK}_{AASigPK}$

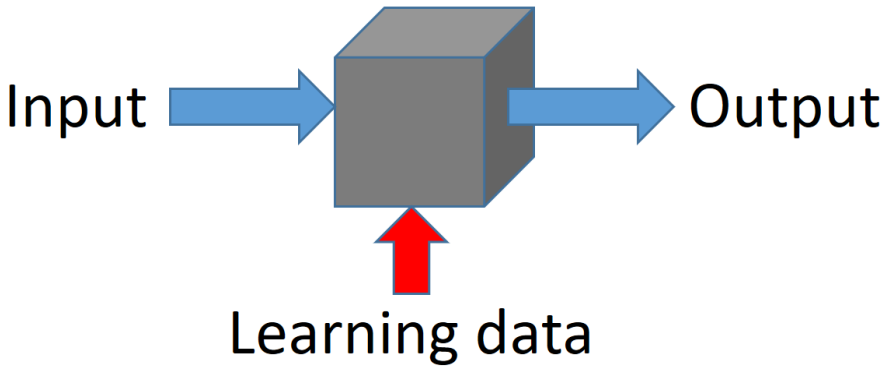
- Common methods to establish **reasonable grounds** for trust in security:
  - security analysis (experts, code analysis, formal methods, verification, ...)
  - security tests (penetration tests, fuzzing tests, ...)

Classic control systems



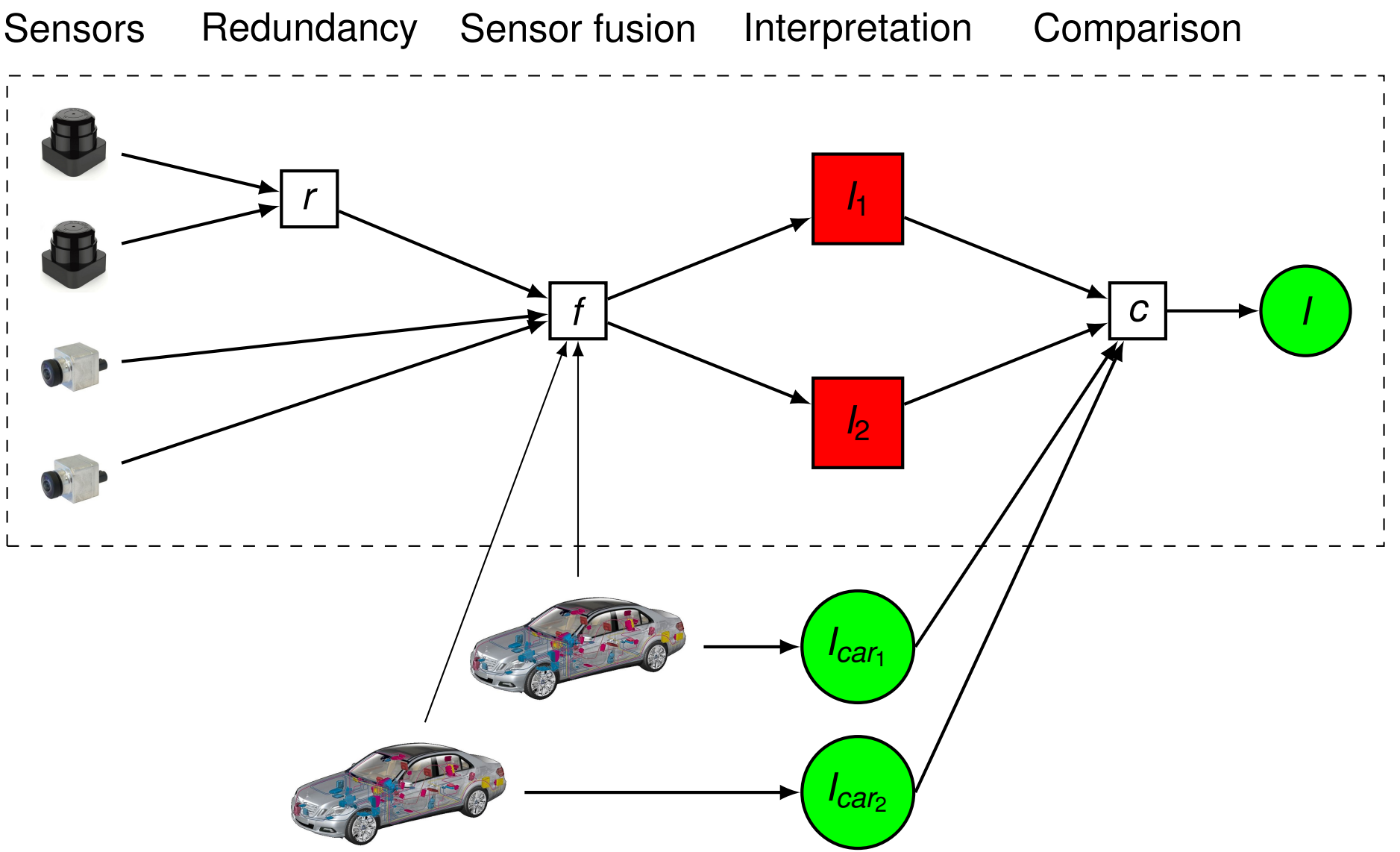
Security analysis of function *F* ✓

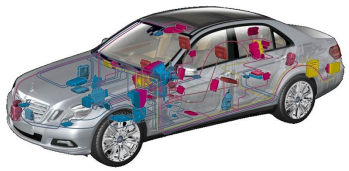
Machine learning control systems



Security analysis of function ???

- Suitable methods for security analysis of machine learning systems are necessary.


Sensors
Redundancy
Sensor fusion
Interpretation
Comparison
r
f
I_1
I_2
c
I
I_{car_1}
I_{car_2}

100 MLOC  $\neq$  40 MLOC

- limited resources (hardware, computing power, network)
  $\rightarrow$ limited applicability of classic security mechanisms
- long duration of use of vehicles (e.g. VW: $\varnothing$ 26 years)[1]
  $\rightarrow$ out-dated HW/SW leading to security weaknesses
  $\rightarrow$ vehicles will need patches and updates (SW & HW)

The security of vehicles needs to be better than the security of PCs.

- more modular and more centralised architecture of IT in vehicles
- more standardised interfaces and components
- methods for verification and testing of security of vehicles

[1] WirtschaftsWoche, 28. Juli 2014, Seite 11

Summary

- Connected (autonomous) vehicles are complex, distributed IT systems embedded in distributed IT systems.
- There is the danger of
  - attacks on communication,
  - attacks on components,
  - attacks on sensors,
  - malicious modification of the environment.
- Specific security measures are necessary to protect vehicles and road users.
- New and improved methods for the analysis and test of security for connected, autonomous vehicles are required.