How Security Mechanisms Can Protect Cars Against Hackers

Christoph Dietachmayr, CIS Solution Manager

EB USA Techday, Dec. 3rd 2015

Elektrobit

EB Elektrobit

Driver´s Fears Are Being Fueled by Recent News

Connected Cars, new opportunies for hackers

IAA: New Autonomous Driving Concepts

EB Elektrobit

Connected Car Offers New Business Models for Hackers?

Autonomous Theft?

Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment

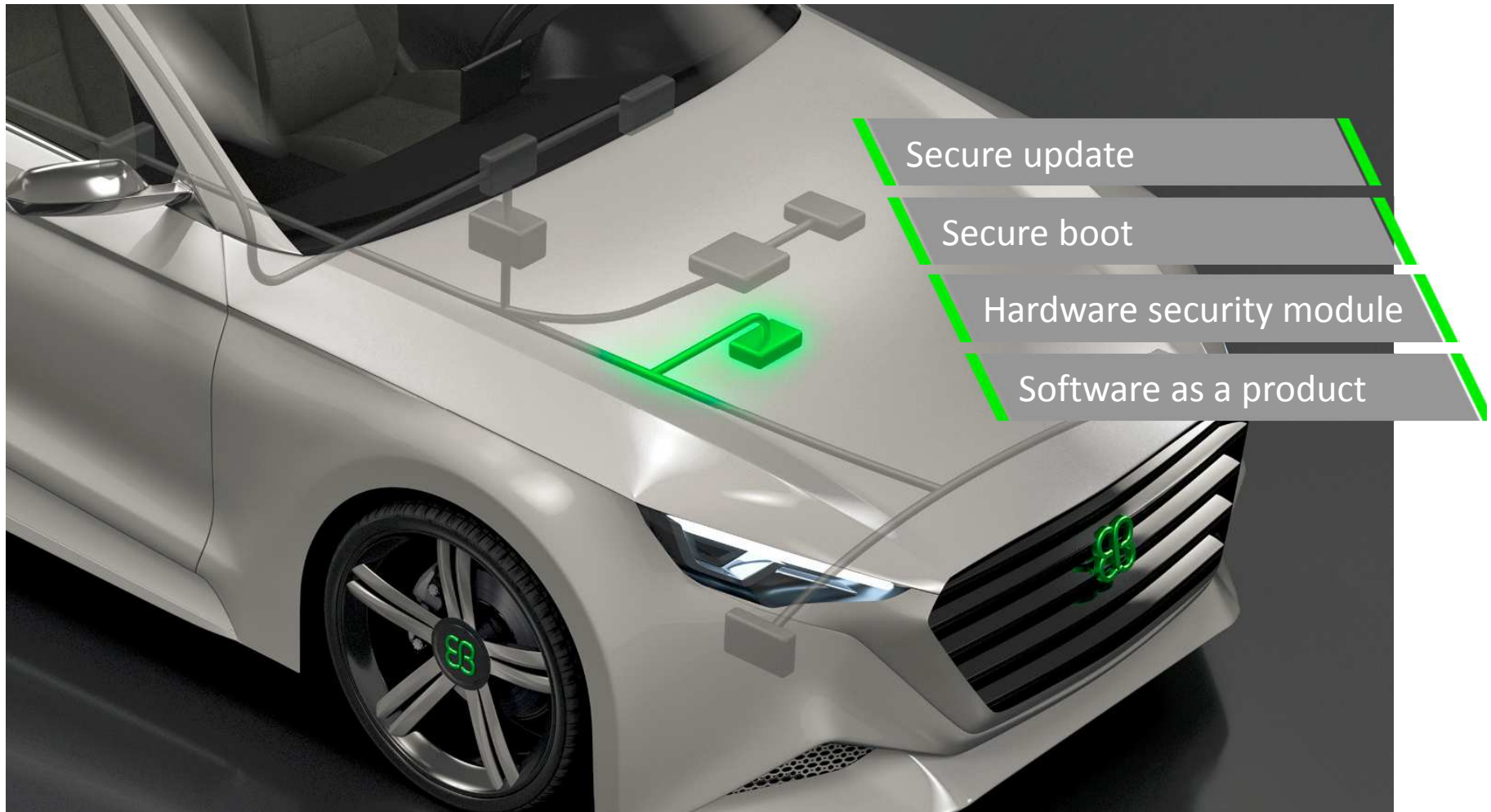- Vehicle Security

- The Connected Car
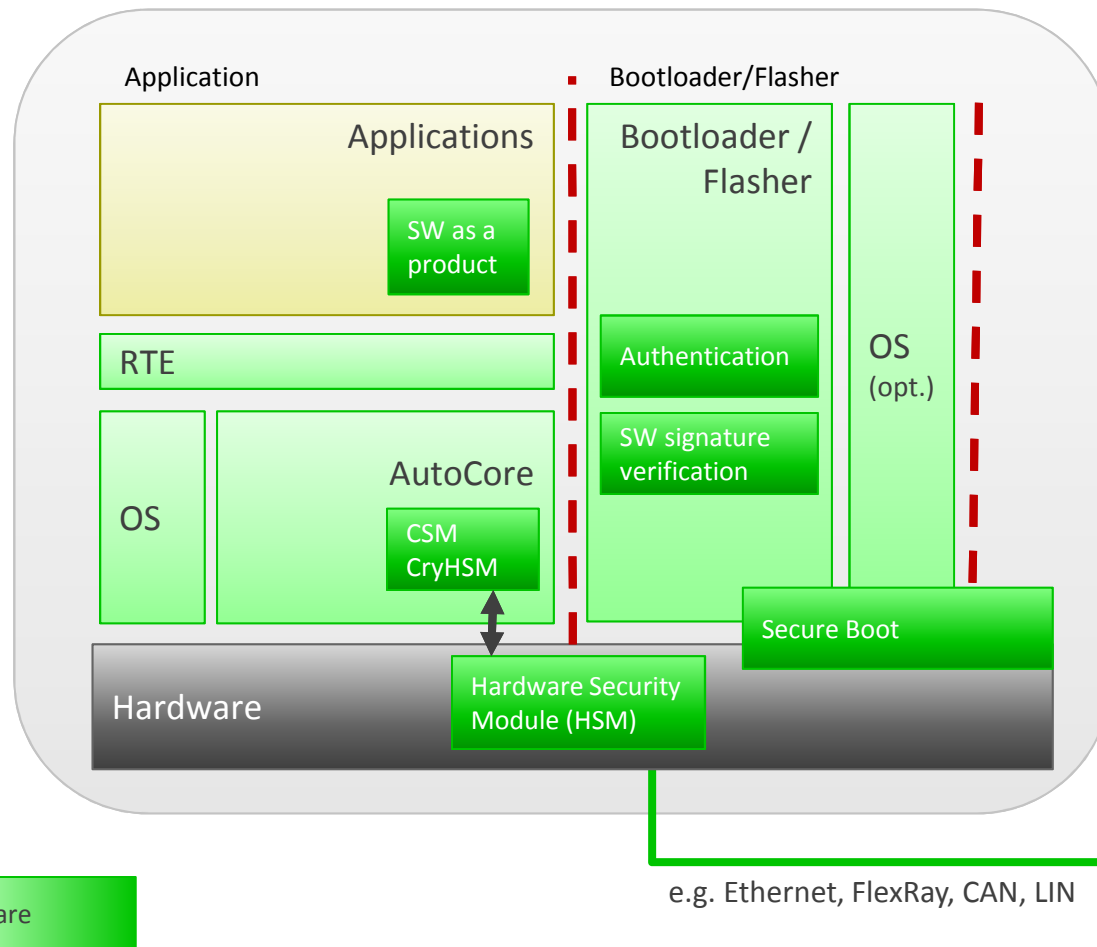
Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment

- Vehicle Security

- The Connected Car

EB Elektrobit
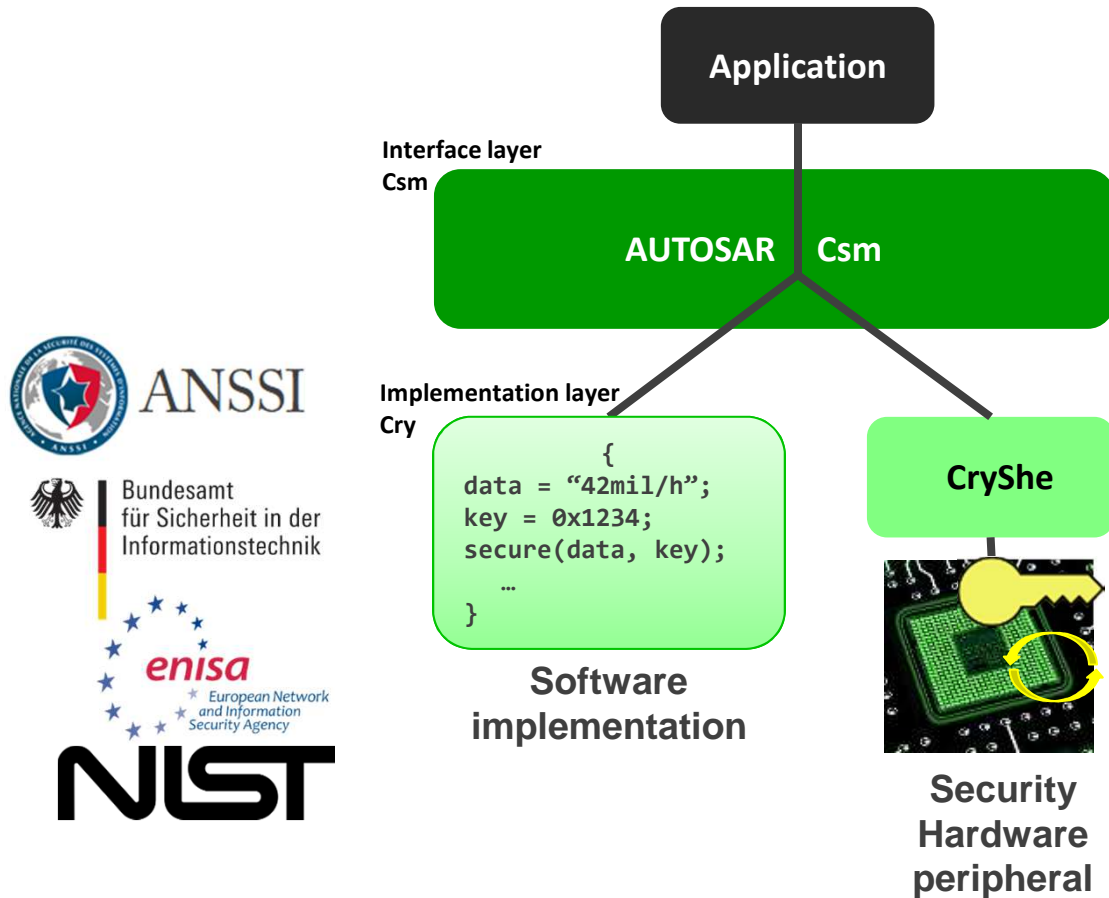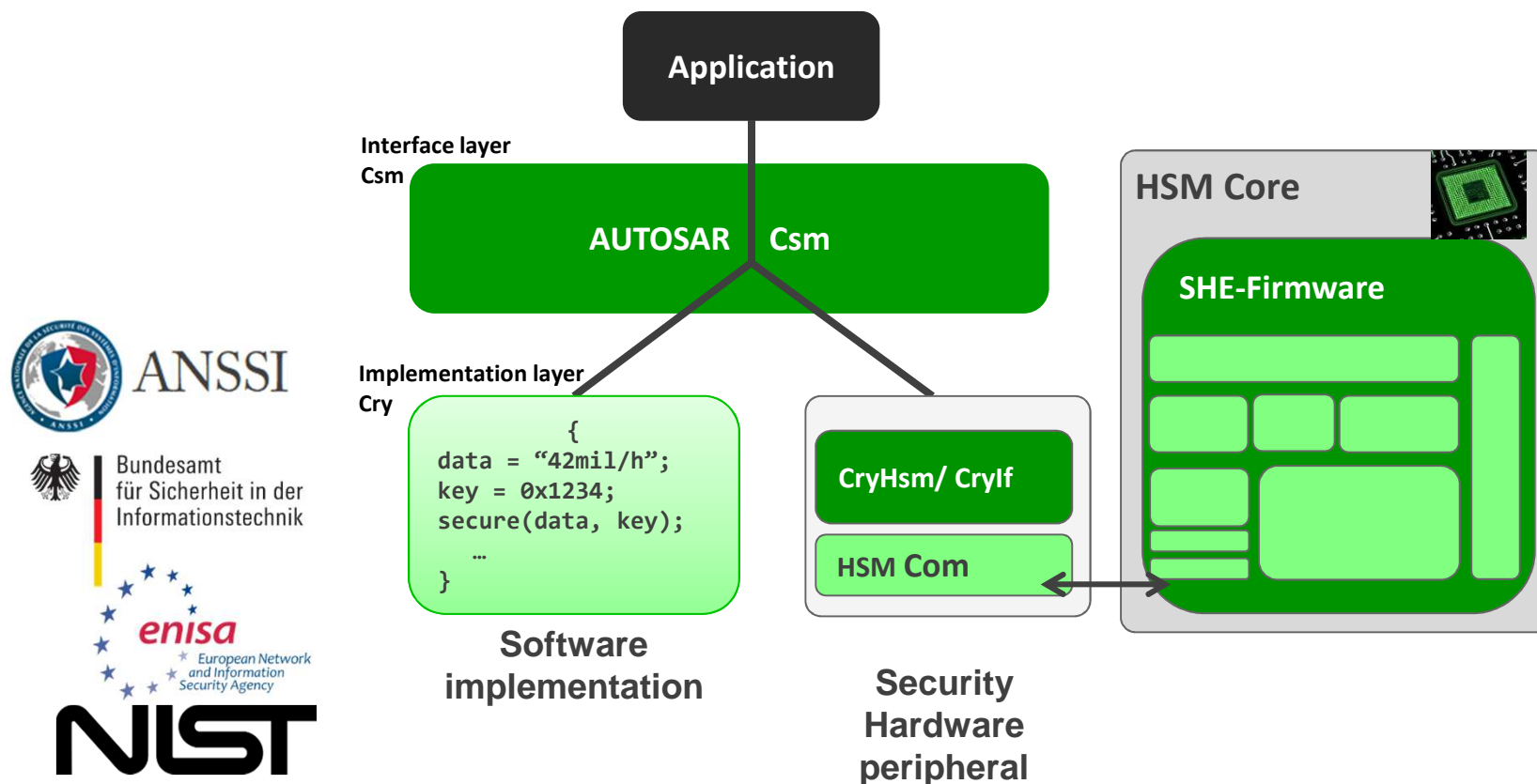
ECU Security

Secure update

Secure boot

Hardware security module

Software as a product

EB Elektrobit

Secure ECU Software Architecture

e.g. Ethernet, FlexRay, CAN, LIN

EB Software

Software and Hardware Security Modules

Application

Interface layer
Csm

AUTOSAR   Csm

Implementation layer
Cry

```
        {
data = "42mil/h";
key = 0x1234;
secure(data, key);
    …
}
```

Software implementation

CryShe

Security Hardware peripheral

Software and Hardware Security Modules

EB supports the algorithms you need!
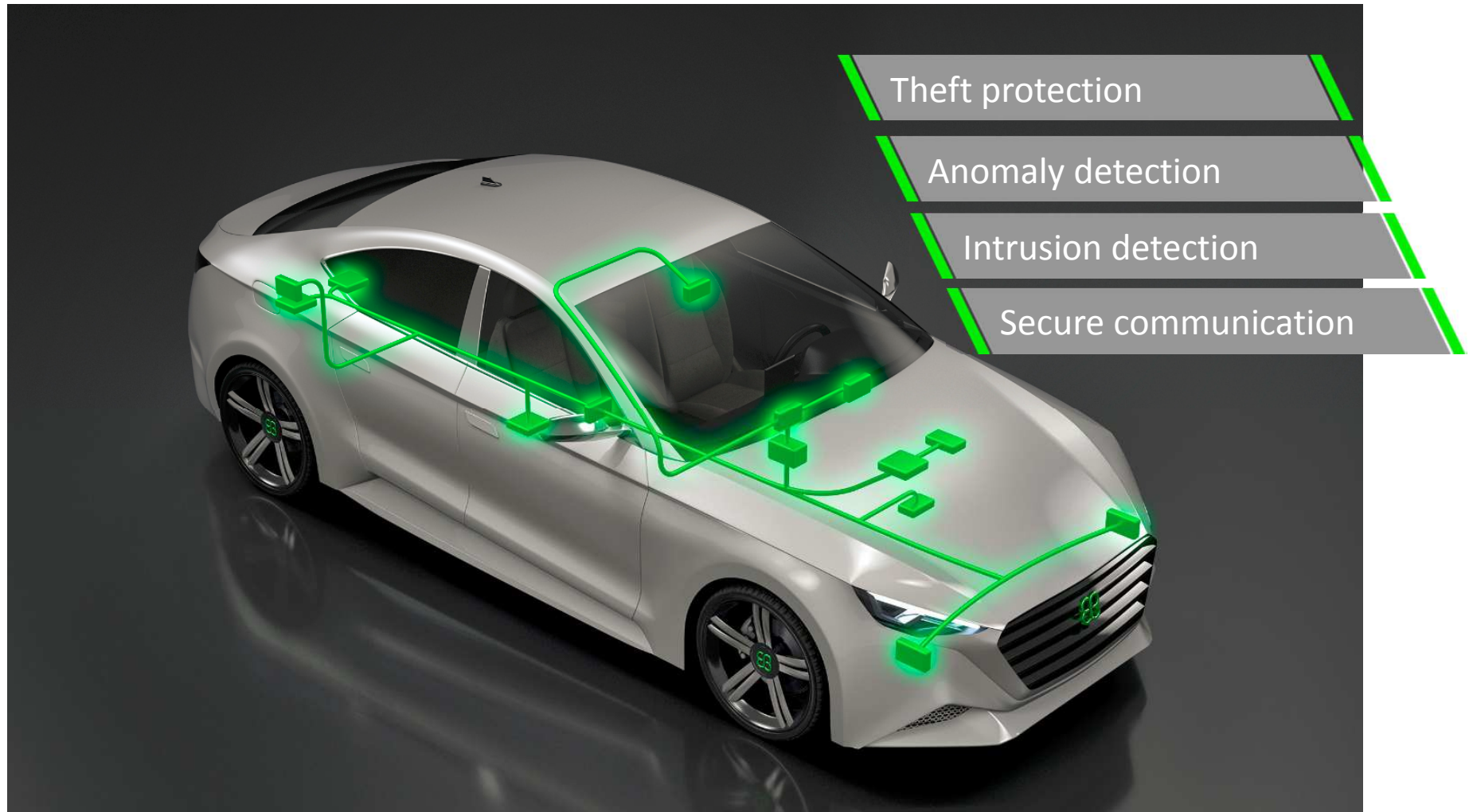
EB Elektrobit

Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment

- Vehicle Security

- The Connected Car

EB Elektrobit

On-Board Network Security

Theft protection

Anomaly detection

Intrusion detection

Secure communication

On-Board Network Security

EB Elektrobit

Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment
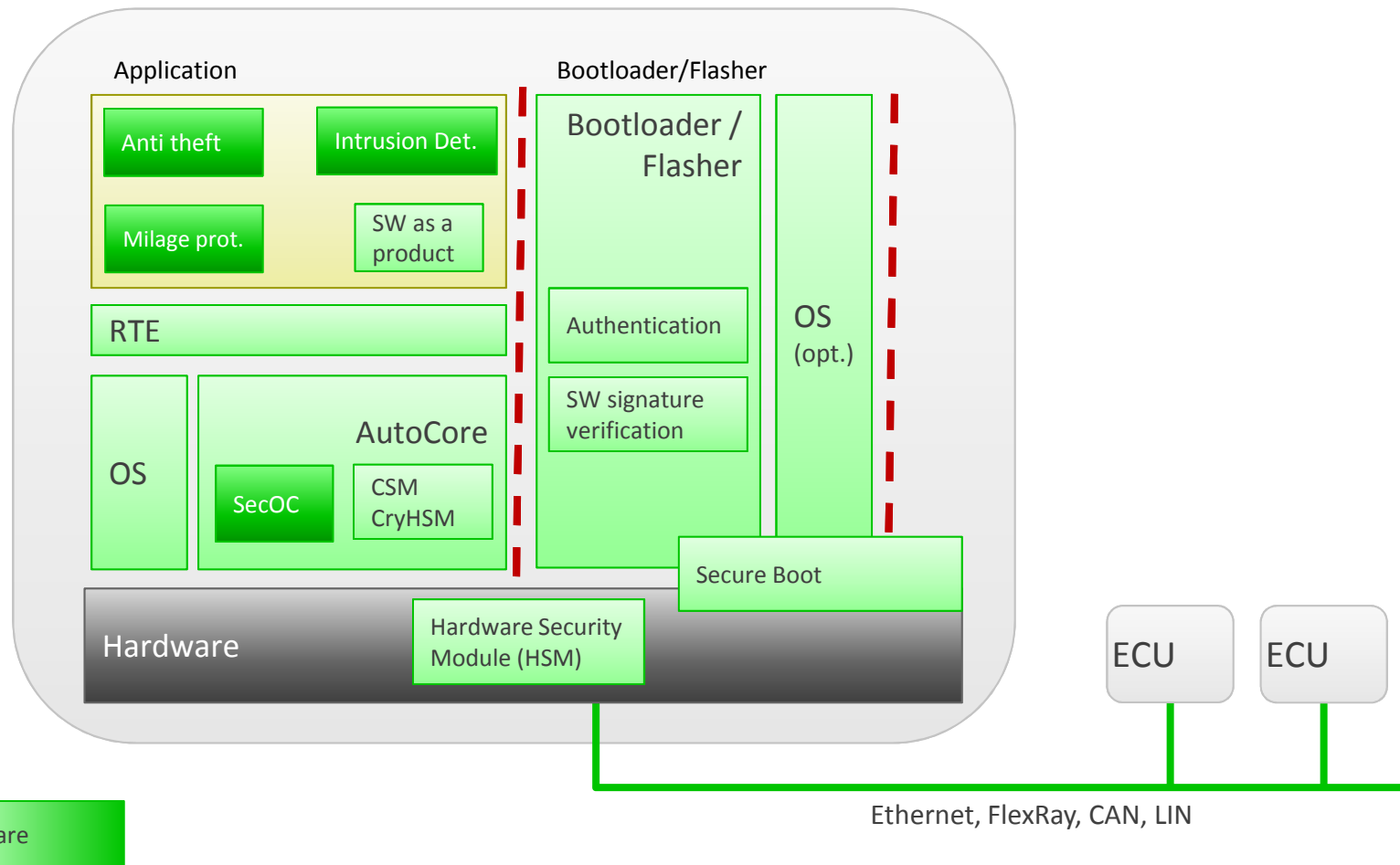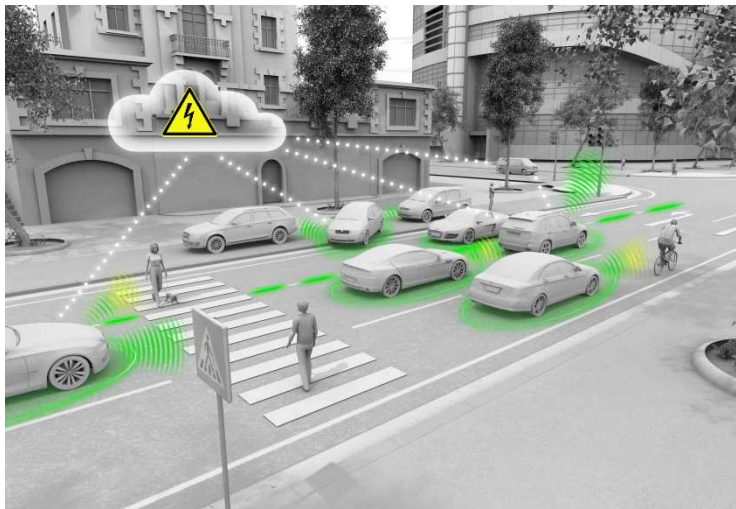
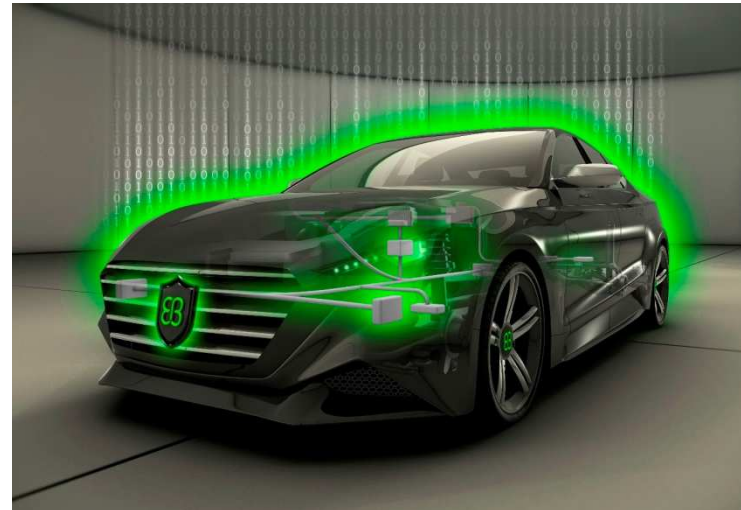- Vehicle Security

- The Connected Car

Security Issues in a Safety Environment

- **Security:** Protection against external access, e.g. hacks

- **Safety:** reliable execution environment for ECUs.
  "knowing what the system does"

Security protects Safety

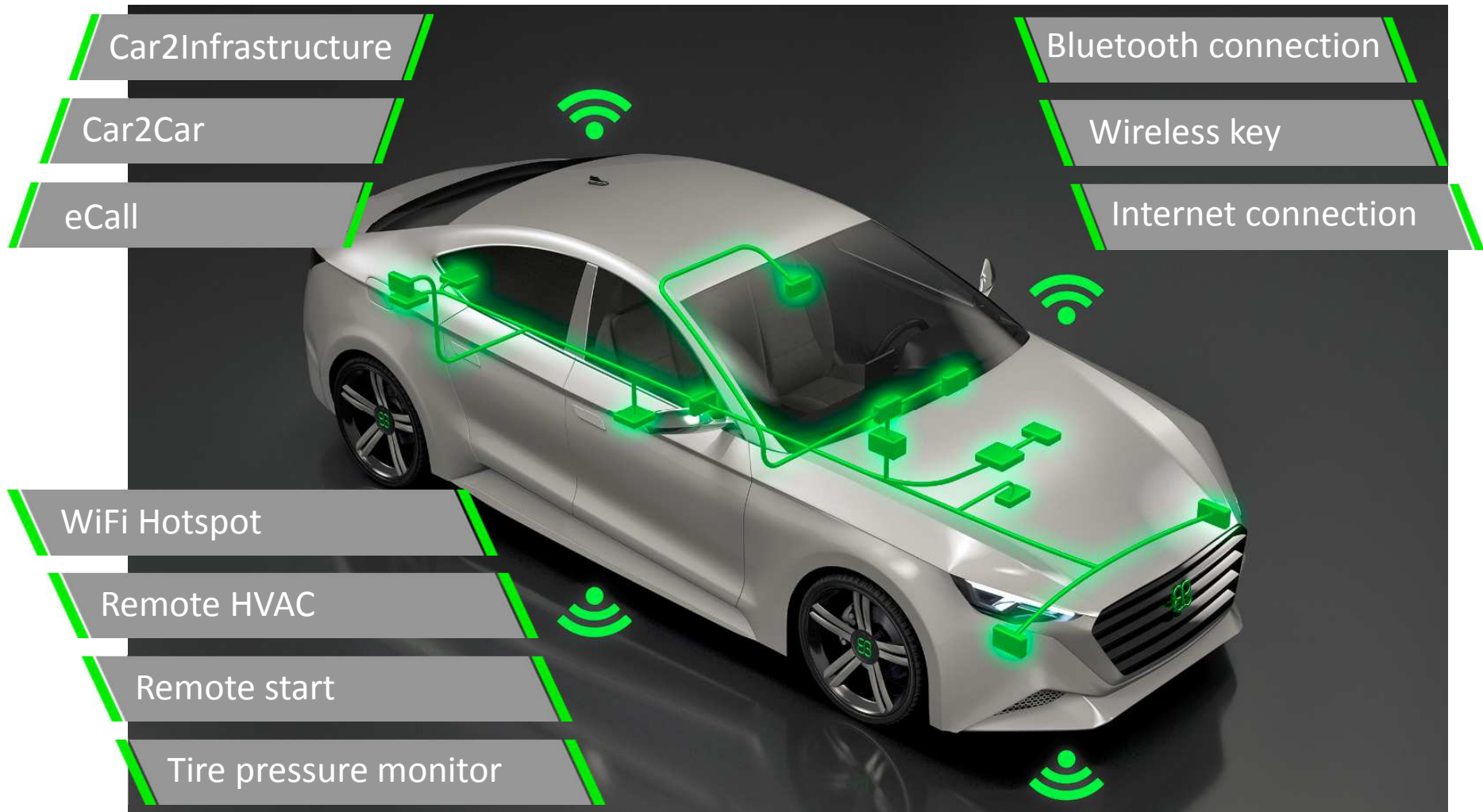**There is no safety without security and vice versa**

EB Elektrobit

Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment

- Vehicle Security

- The Connected Car

Vehicle Security: Various Access Points

Car2Infrastructure

Car2Car

eCall

Bluetooth connection

Wireless key

Internet connection

WiFi Hotspot

Remote HVAC

Remote start

Tire pressure monitor

Current Vehicle Systems Architecture

Future Vehicle Systems Architecture

EB Elektrobit

Use Case: Smart Antenna

Smart Antenna
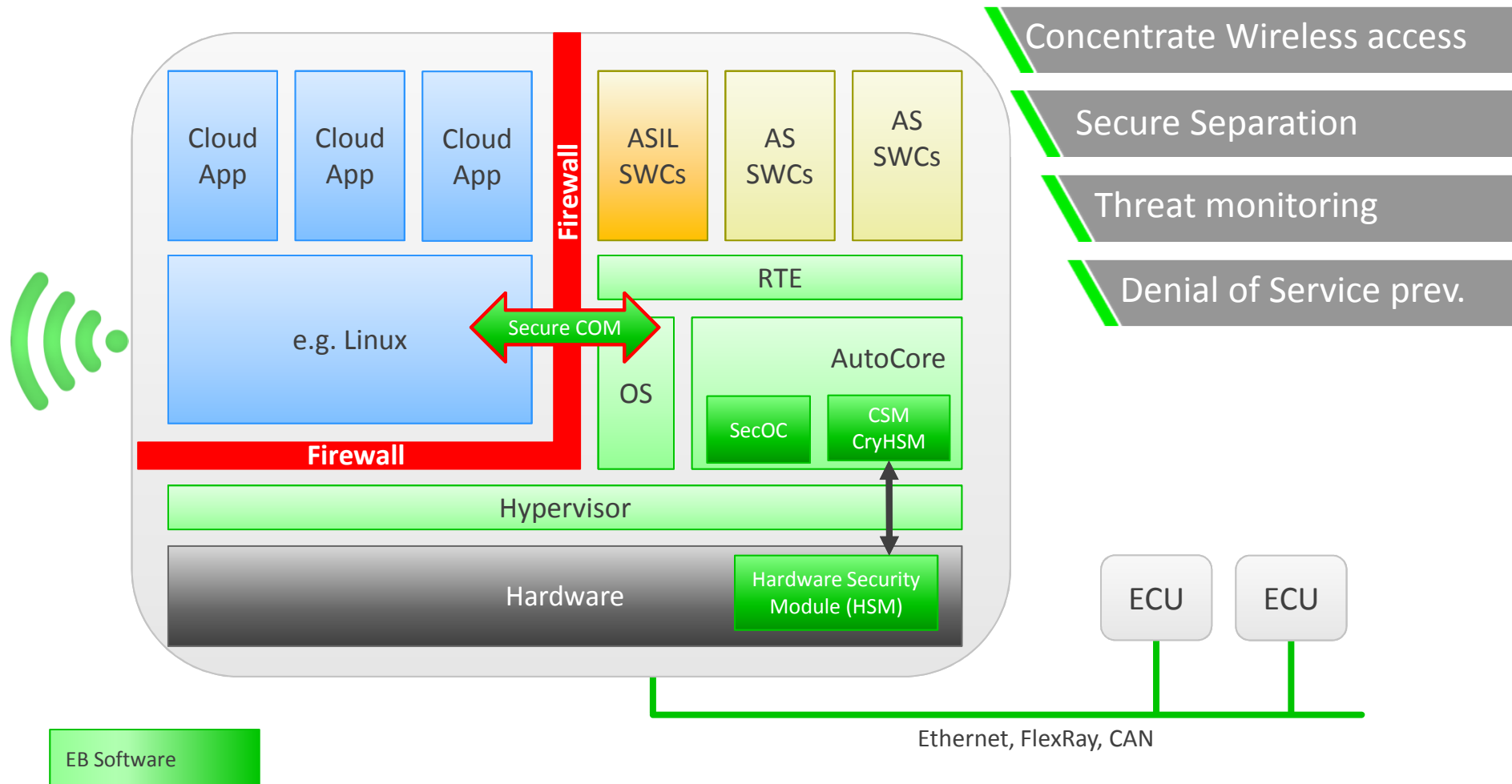
EB Elektrobit

Vehicle Security

Elektrobit

Agenda

- Electronic Control Unit (ECU) Security

- On-board Network Security

- Excursion: Security Issues in a Safety Environment
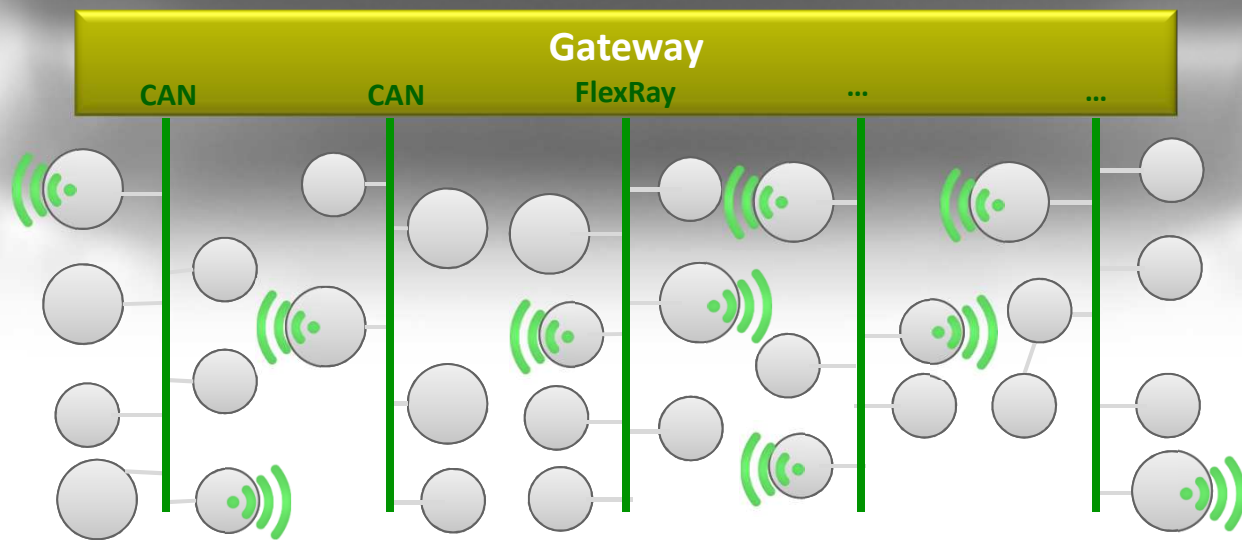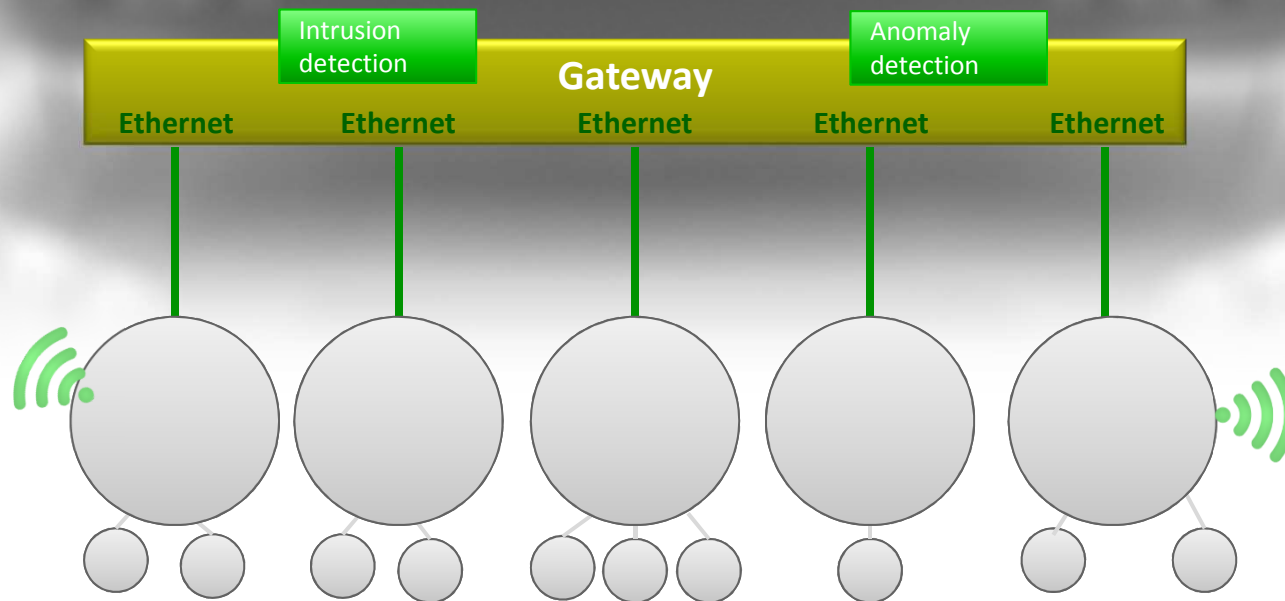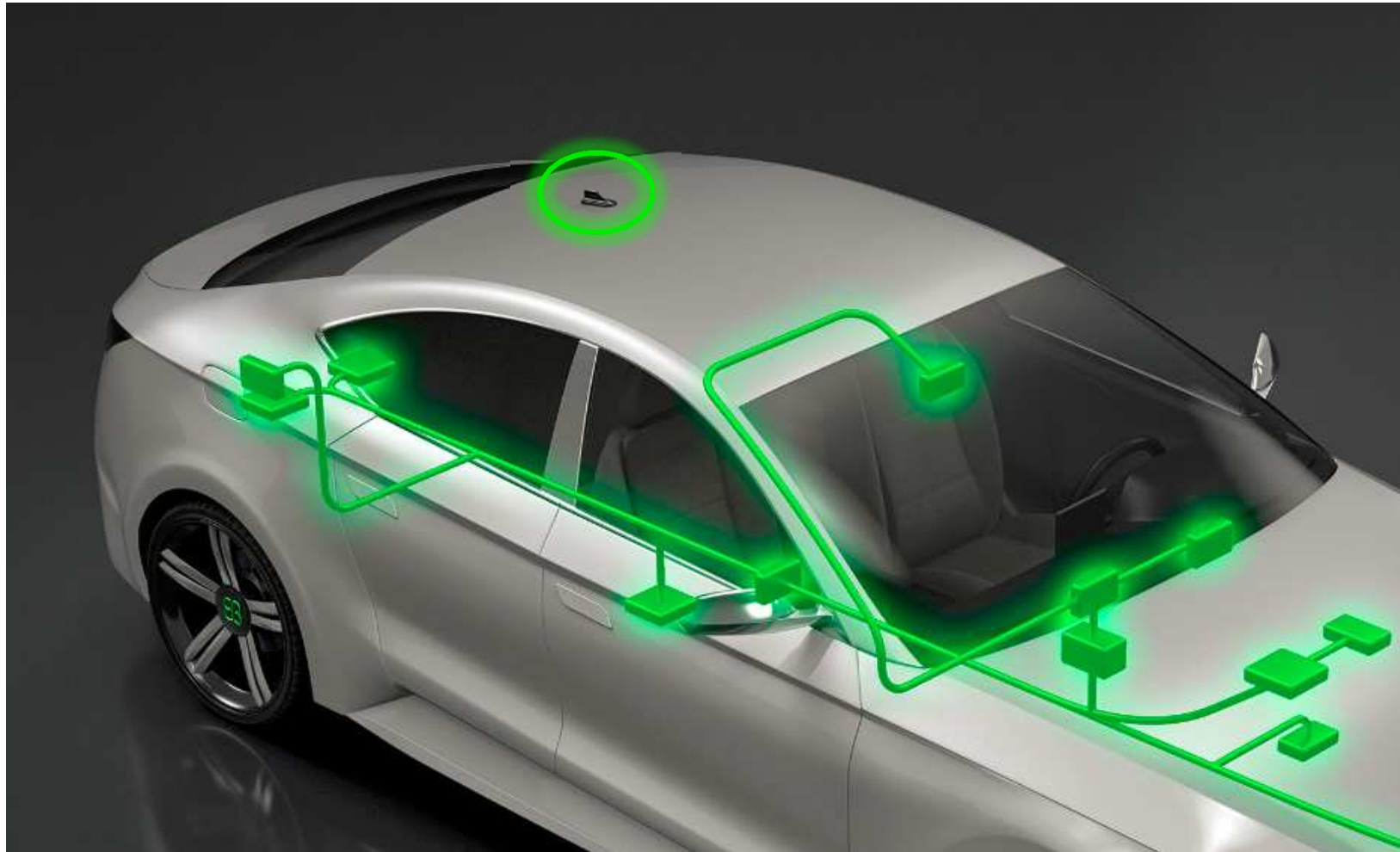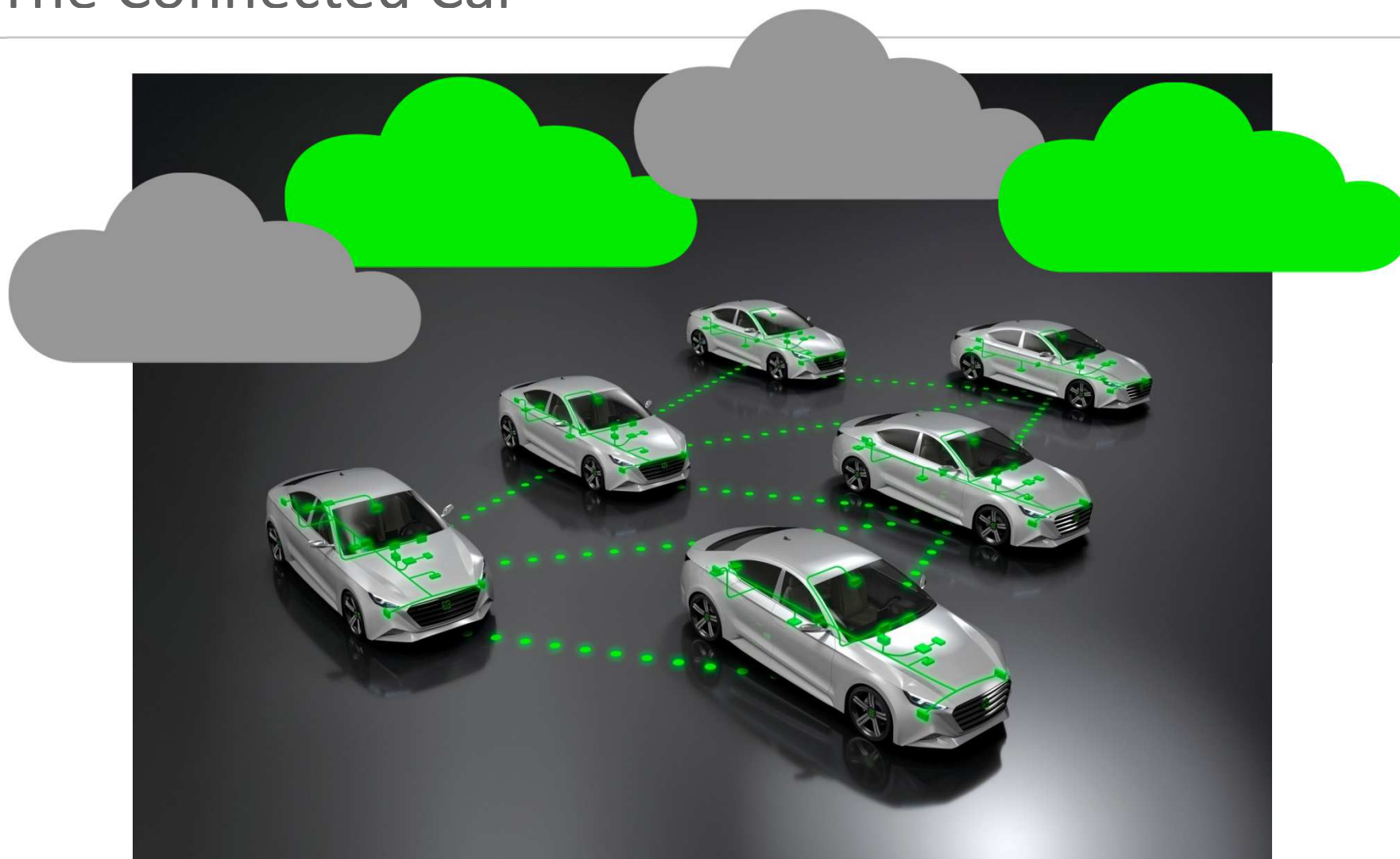
- Vehicle Security

- The Connected Car

The Connected Car

The Connected Car

The Connected Car

The Connected Car

EB Elektrobit
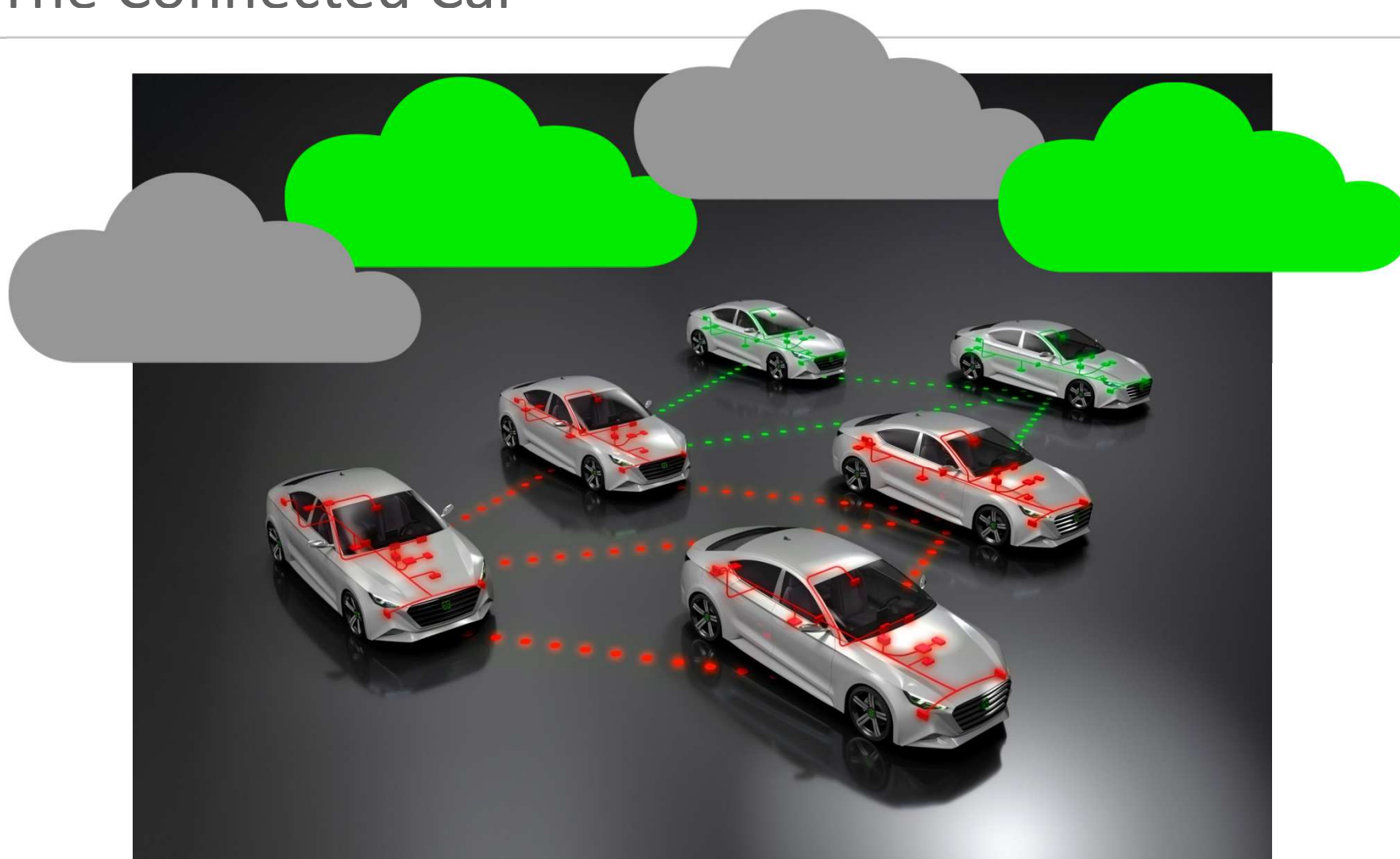
Over the Air Functionality

- Secure Backend Channel
- SW storage
- Firewall
- Secure COM
- Over the Air:
  - SW update agent
  - Remote Diagnostics agent
  - …
- Firewall
- Hypervisor
- Hardware
- Hardware Security Module (HSM)
- Target ECU
- Target ECU
- Ethernet, FlexRay, CAN

100% security is an illusion

Secure OTA update

Remote diagnostics

Identity vs. privacy

EB Software

EB Security Portfolio

AES, RSA, ECC,…

Secure separation
- Hypervisor
- Virtualisation

Crypto
- Algorithms
- SHE drivers
- HSM drivers

Secure HW
- HSM firmware
- Future Security HW
- Security architecture

OTA
- Secure Connection
- Update strategies
- Implementation
- Backend

Security applications
- Unlock / Download
- SW as Product
- Secure Com …

Testing & Certification
- Functional
- Penetration Testing
- FIPS / Com. Criteria

Key management
- Sym/Asym
- Key Derivation
- Initial / Update

Secure Communication
- Firewall
- Intrusion-/Anomaly detection

Security Consulting
- Architecture
- Solutions
- How-To

Car2X
- Consulting
- Implementation
- Testing

Summary

- **Security is necessary on all levels**
  - In ECUs and between ECUs
  - In the vehicle and between vehicles
  - In the backend

- **A big challenge, but you are not alone**
  - Existing and approved mechanisms available
  - EB secures vehicles for more than 15 years

- **Security needs constant care**
  - Monitoring on all levels
  - Update over the air is key to keep cars secure

- **Visit us at: https://www.elektrobit.com/security**

Thank you

EB Elektrobit

Christoph.Dietachmayr@elektrobit.com
automotive.elektrobit.com