End-to-end security for connected vehicle architectures

Jochen Olig

21 Febbraio 2019, 16° Workshop di Automotive SPIN Italia - CRF Orbassano (TO)

Elektrobit

EB security solutions

Do connected cars offer new business models for hackers?

EB security solutions

Autonomous theft?

Trusted protection

PREVENT

Make it as hard
as possible to attack

UNDERSTAND

Know you are being
hacked and how,
in real time

RESPOND

Mitigate the damage and
immunize the fleet in hours

Trusted protection

PREVENT

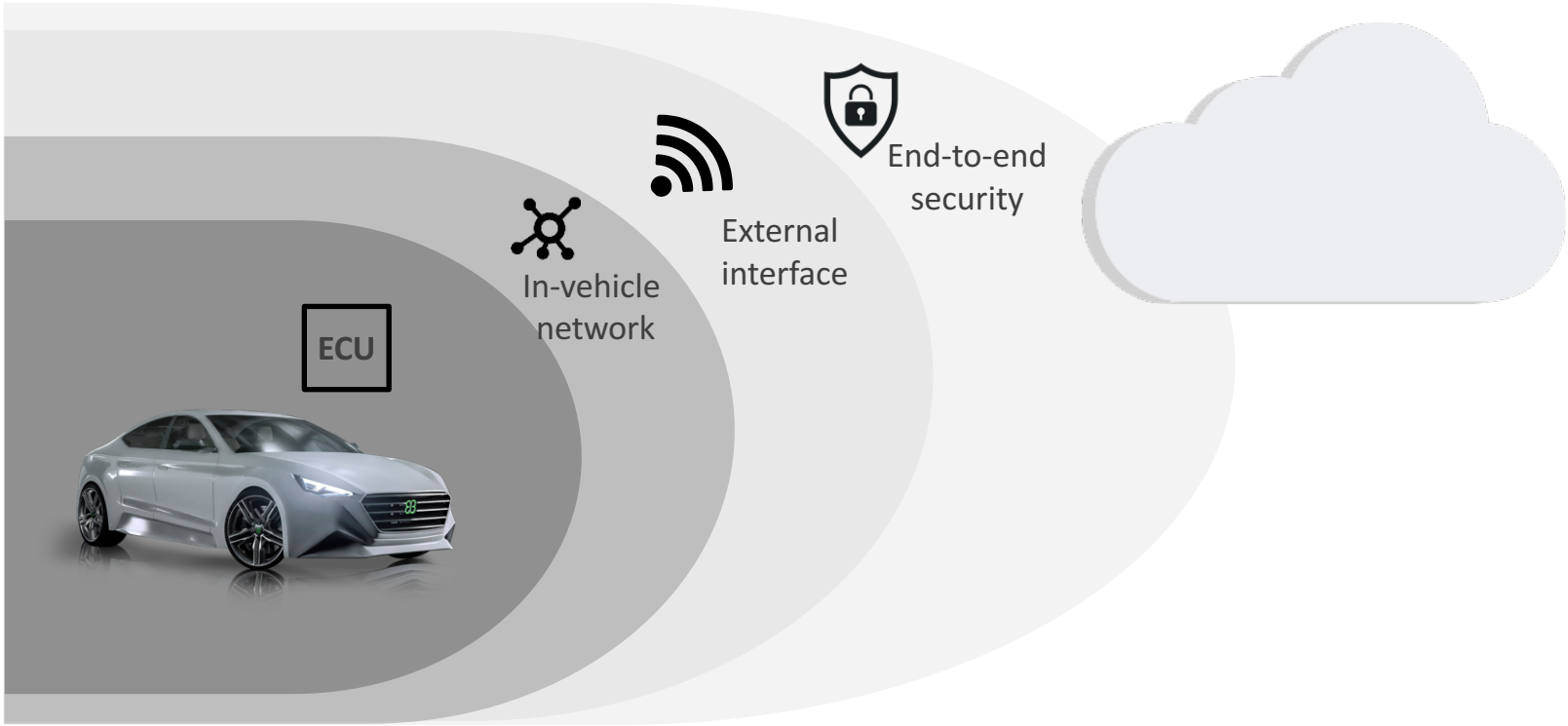
Make it as hard
as possible to attack

- Hardware enhanced crypto
  - SHE, HSM
- Embedded security software
- Secure networks
  - SecOC
  - TLS
  - IPSec
- Secure vehicle architecture
  - Secure and unsecure zones
  - Redundancy of secure zones

Elektrobit

ARGUS

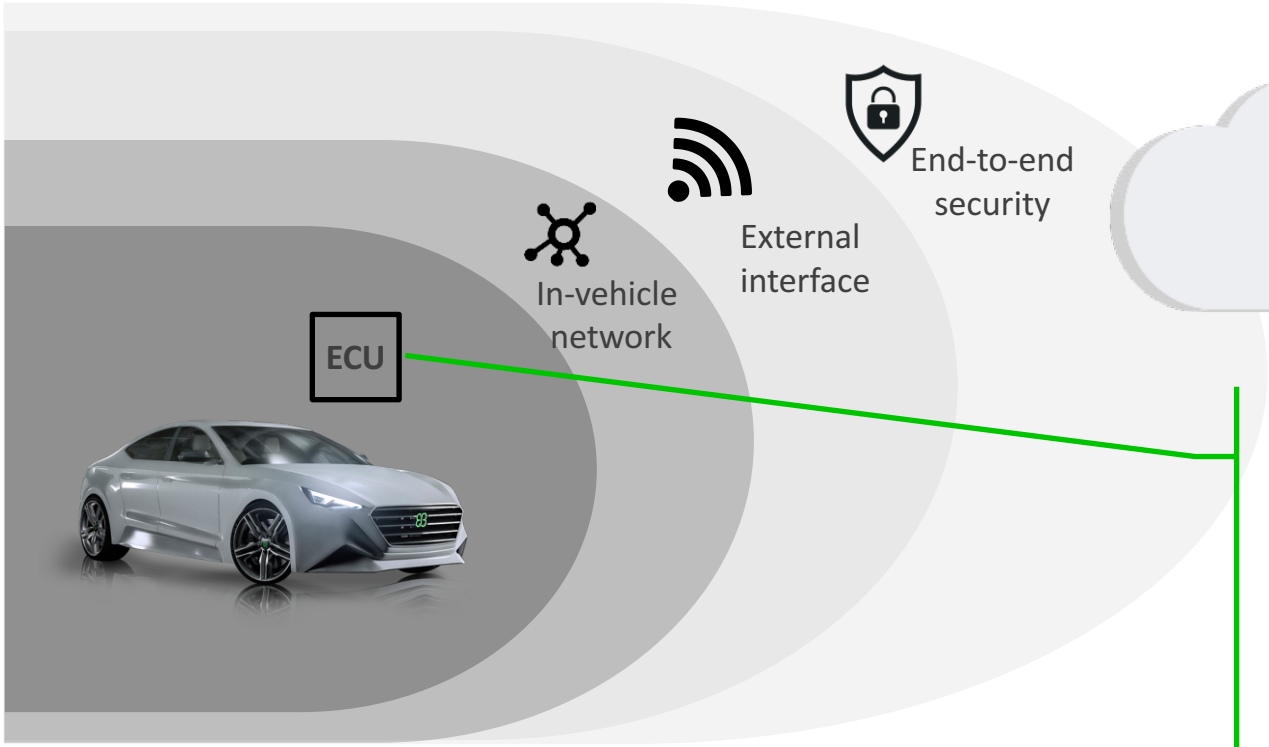
Security layers for connected cars



Elektrobit

ARGUS

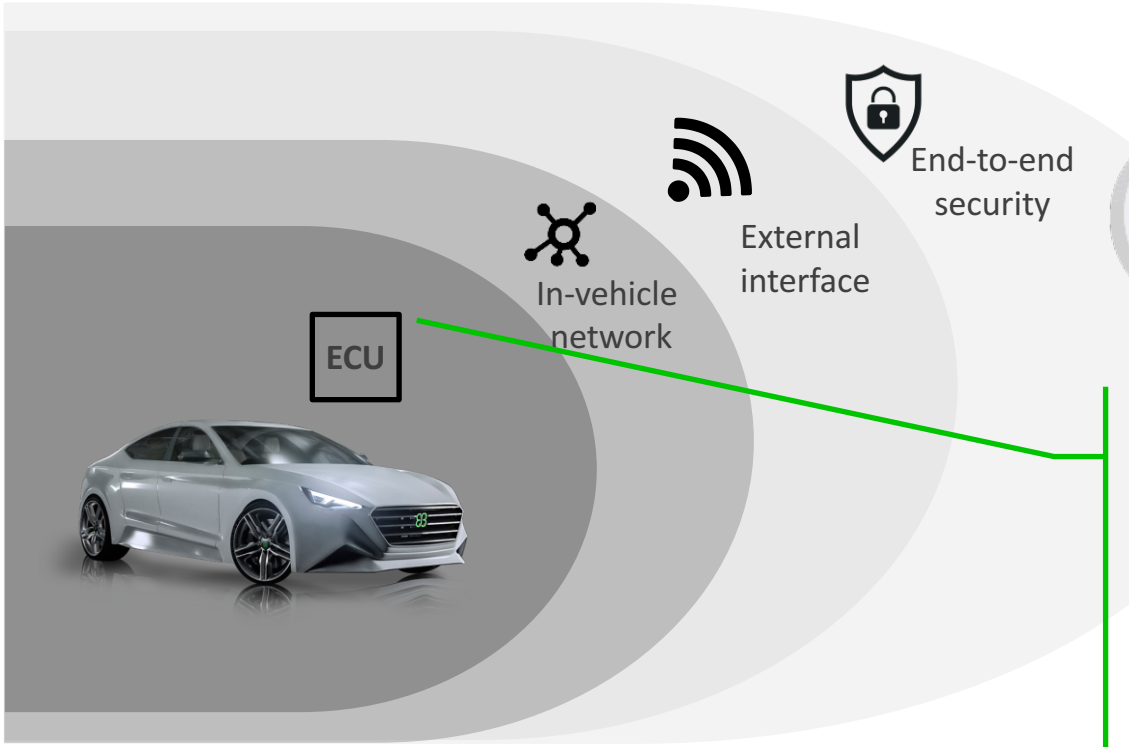
Security layers for connected cars



Protection of single ECUs

- Flash protection
- Software-enabling
- Secure Hardware Extension (SHE)
- Hardware Security Module (HSM)
- Secure Boot
- Separation/Isolation
- Secure Diagnostics

Security layers for connected cars



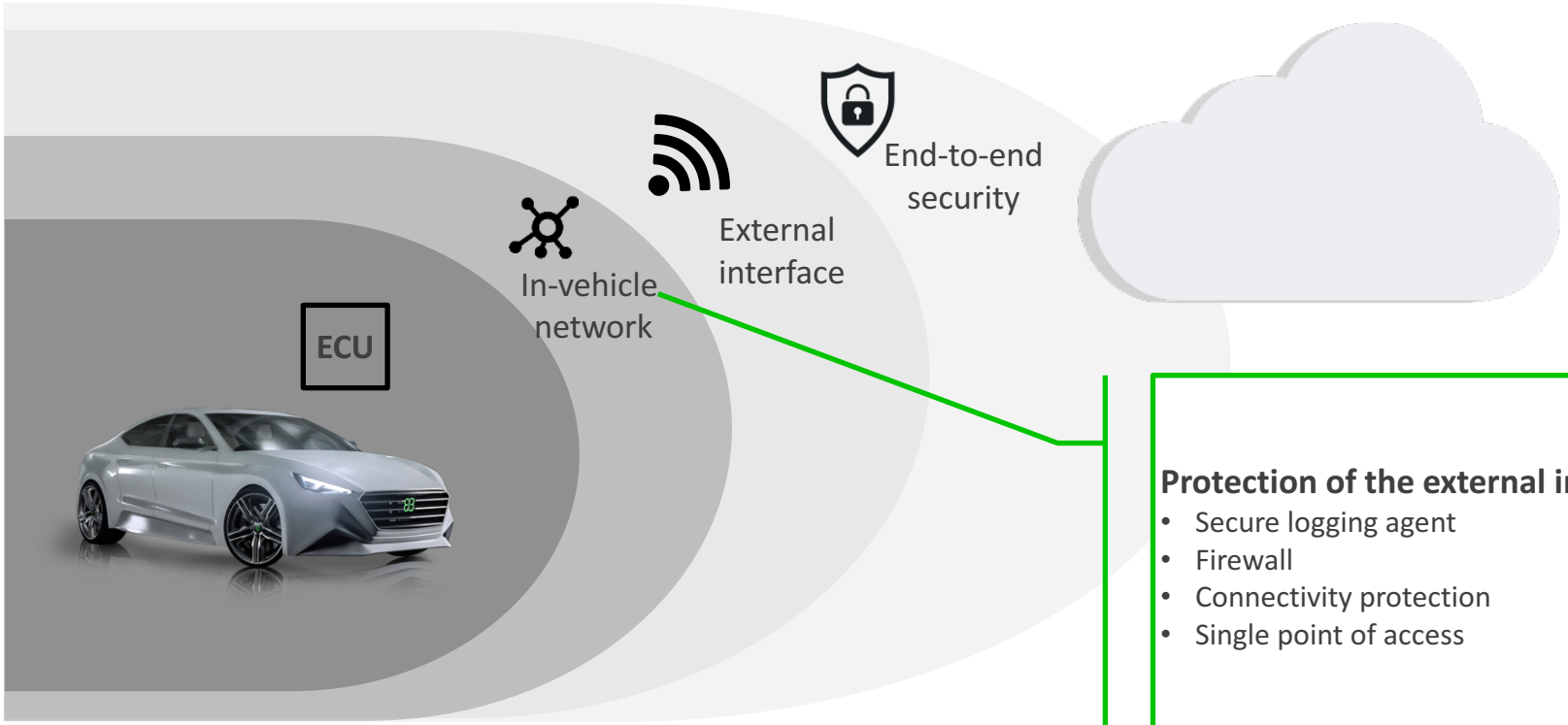
Protection of the in-vehicle network

- Secure on-board communication
- Ethernet Security (TLS, IPSec)
- IDS
- Domain separation
- Anti-theft protection

Elektrobit

ARGUS

Security layers for connected cars



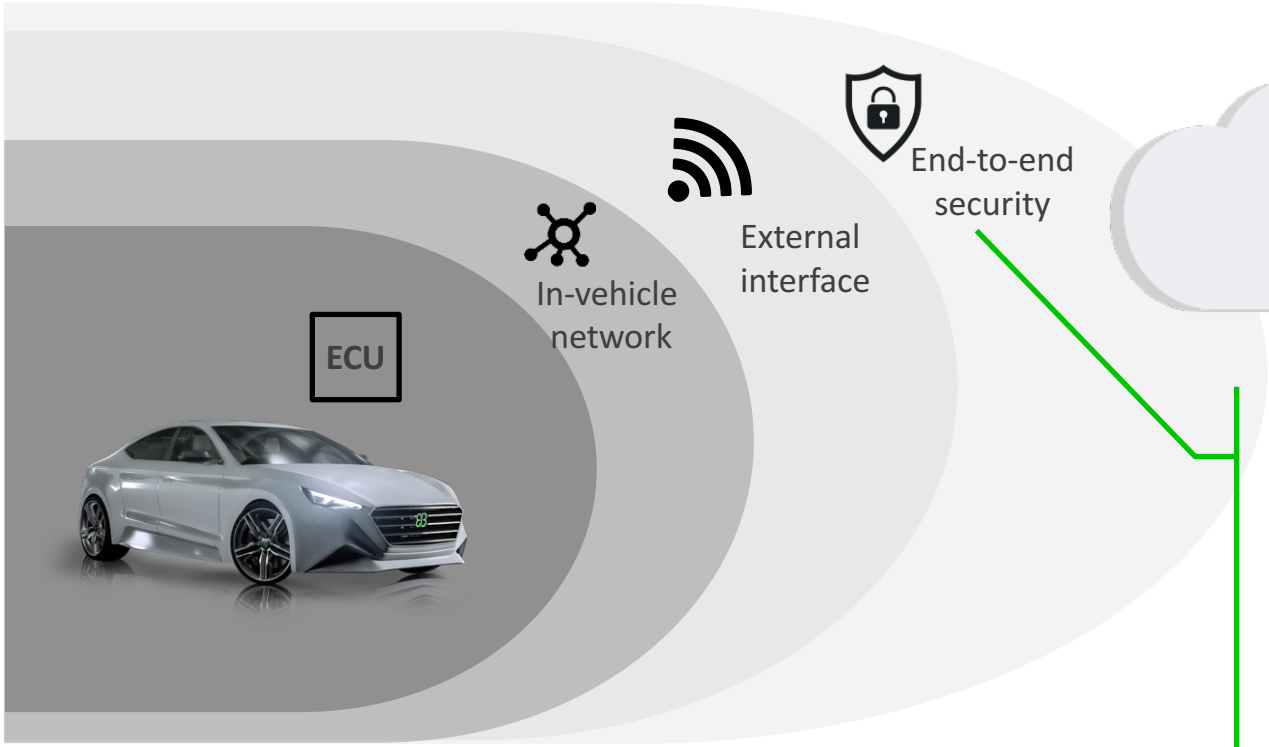
Protection of the external interfaces

- Secure logging agent
- Firewall
- Connectivity protection
- Single point of access

Elektrobit

ARGUS

Security layers for connected cars



Protection over lifespan

- Secure channel to the backend

⇒ Mutual authentication

⇒ Tap-proof

- Secure backend infrastructure

HSM as the root of trust

End to end protection needs a root of trust in hardware

HSM (Hardware Security Module)

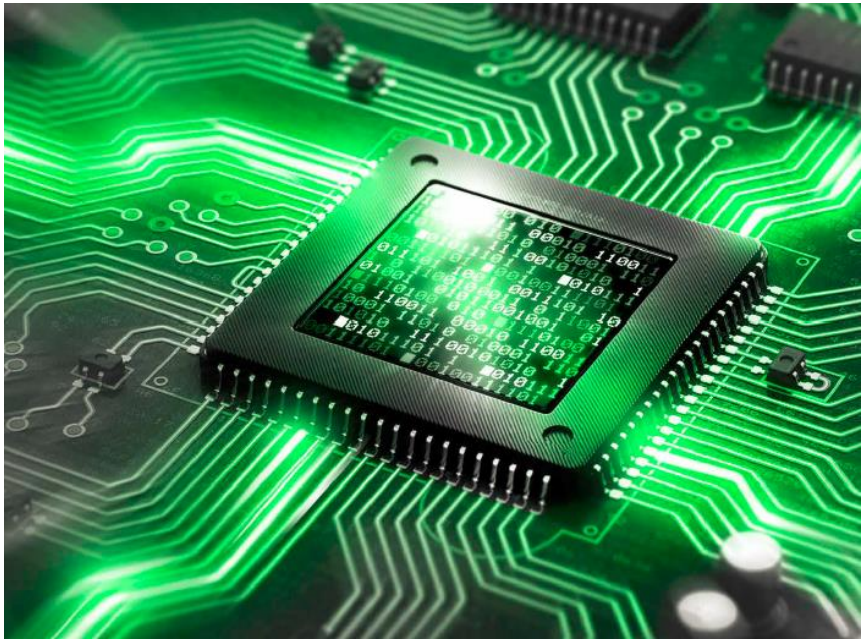
- Onchip coprocessor
- Key generation, storage, management
- Acceleration of cryptographic algorithms

HSM firmware:

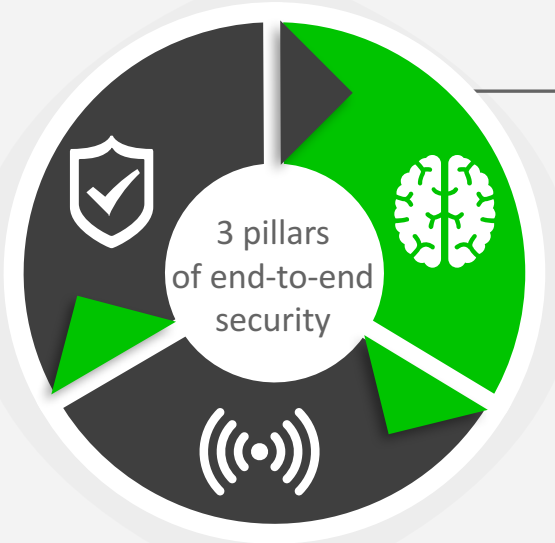
- Enables the use of a hardware module (HSM)
- Implementing security algorithms utilizing hardware acceleration mechanisms

Security benefits:

- Parallel execution of cryptographic calculations
- Accelerated cryptographic calculations
- Hardware trust anchor



Trusted protection



UNDERSTAND

Know you are being
hacked and how,
in real time

- Cyber security fleet monitoring
- Cyber security analysis

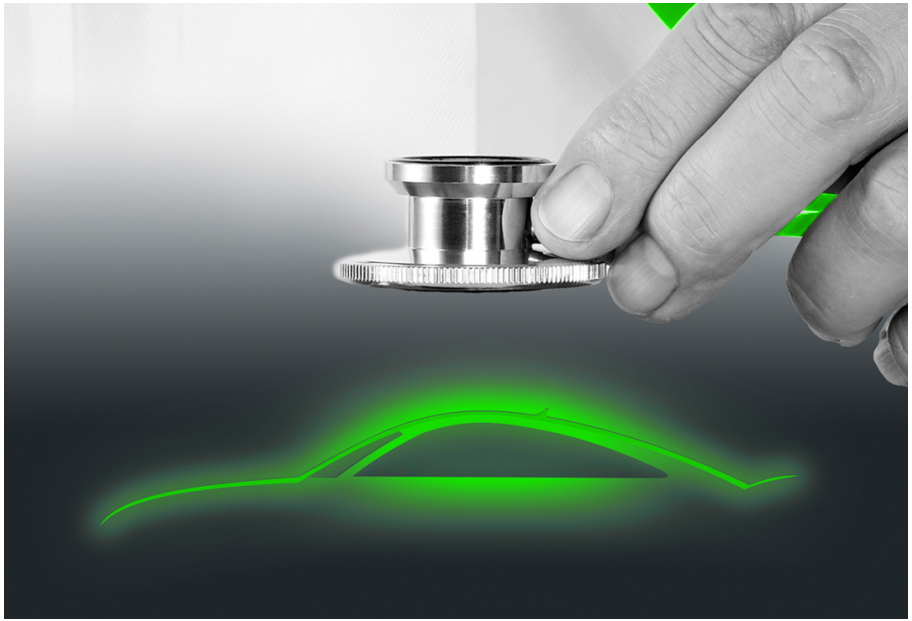
Leverage existing data („Security Monitor“)

Highlights

- Leverage data already existing in a car, e. g.
  - failed verification attempts for SecOC
  - DTCs like „memory section violation“
- Combine and aggregate the data pool in the car
- Provide the information in a standardized way for further processing in the backend

Benefits

- Get insights from your vehicles on the road
- Automation of data collection in the car
- Smart integration in existing intrusion detection or monitoring functionalities



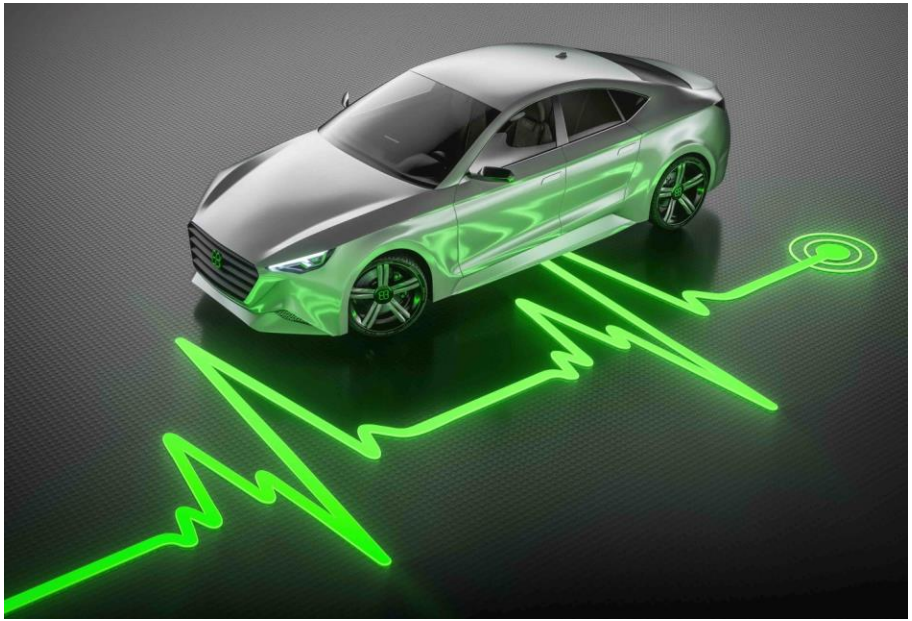
Remote analytics tool for connected cars

Highlights

- Create customizable and configurable jobs (surveys, remote diagnostics) to gather data
- Gathered data is sent to backend for analysis
- Permanent surveillance or ad-hoc surveys possible
- Offline use possible (buffering and upload strategy)
- Reliable, scalable, and secure

Benefits

- Get insights from your vehicles on the road
- Automation of data collection
- Allows predictive maintenance, root cause analysis, monitoring new SW versions



Intrusion Detection and Prevention – IDPS

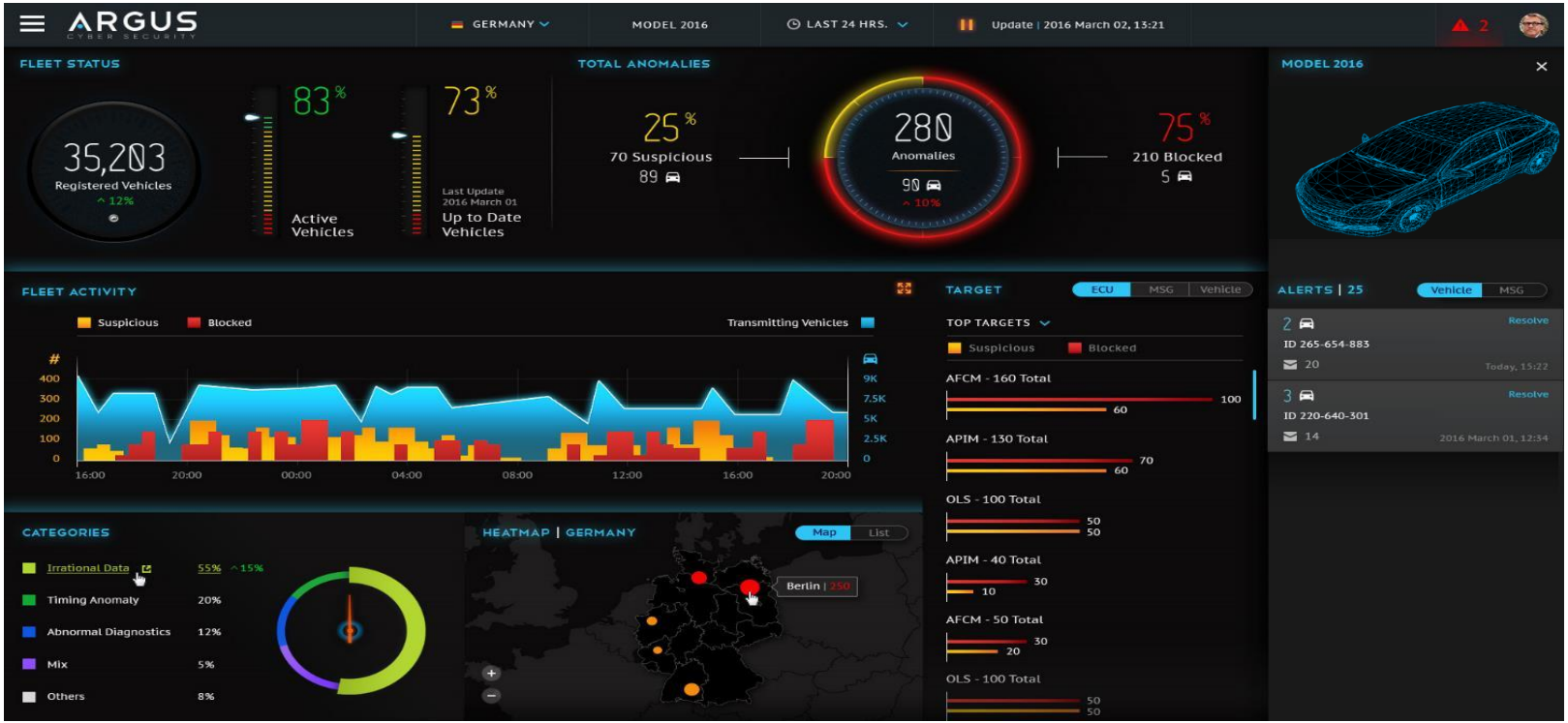
Monitoring In-Vehicle Network to detect and block cyber attacks

- Analyzing network traffic for deviations
- Detects attacks, suspicious activity and changes in standard in-vehicle network behavior
- Rule-set based, specifically generated (off-line) for a vehicle
- Rule-set reflects vehicle traffic in normal operation
- Deviations are detected and logged
- Local autonomous in-vehicle detection
- Cross fleet analysis in the cloud

Examples of what can be detected

- Violations of network specifications
- Denial of service attacks
- Confliction attacks (overriding existing signals)
- Out of context messages
- Diagnostic attacks
- Advanced use cases – FOTA and SecOC manipulations

Intrusion and Anomaly detection



Trusted protection

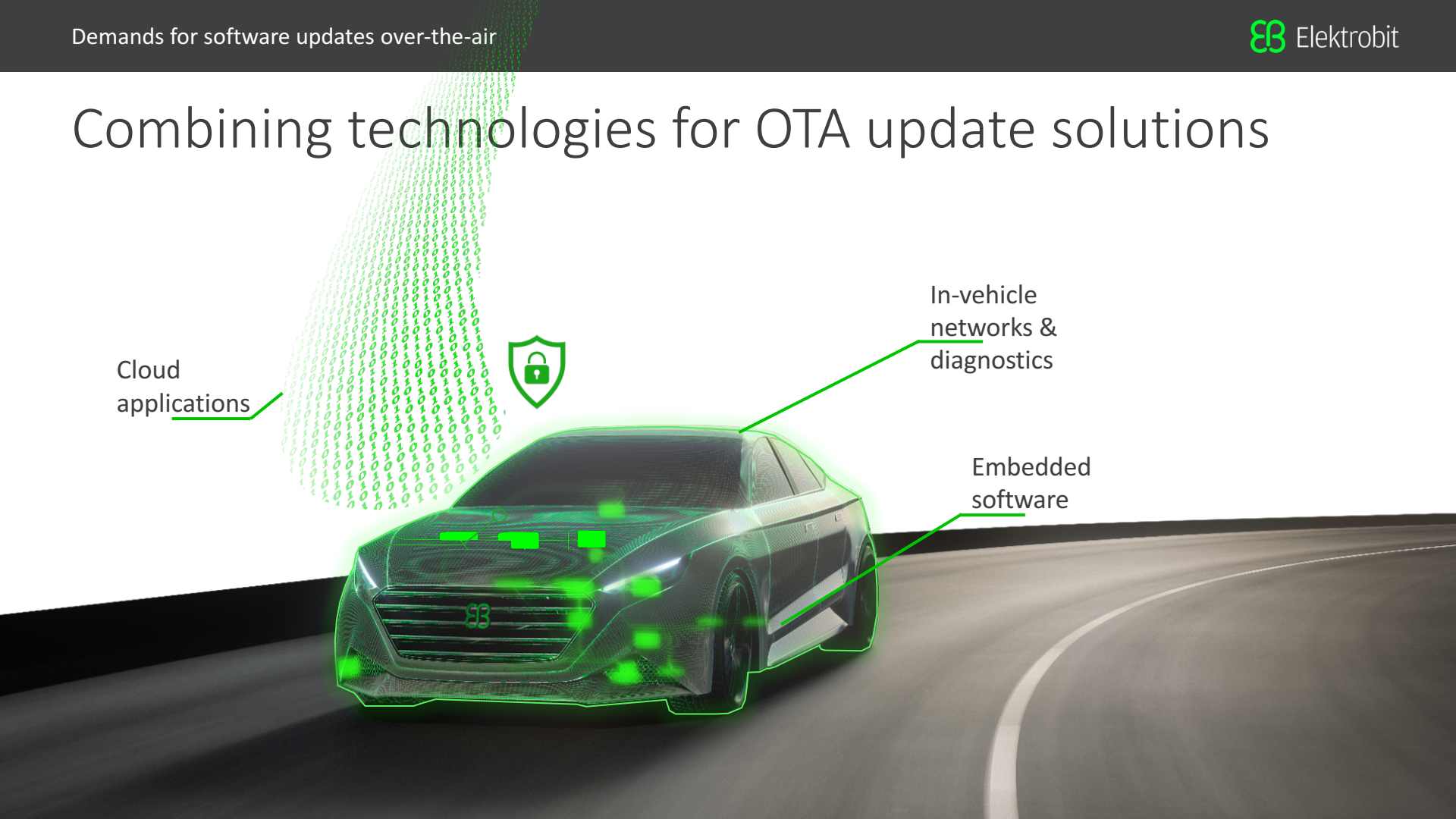
RESPOND

Mitigate the damage and immunize the fleet in hours

- Policy/rule set update
  - Fast response
  - Attack mitigation
  - Win time
- Software updates over-the-air
  - Erase root cause

Elektrobit

Combining technologies for OTA update solutions



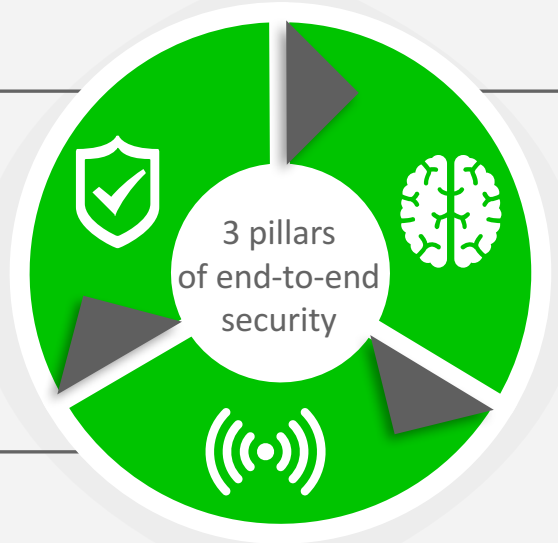
Trusted protection

PREVENT

Make it as hard
as possible to attack

UNDERSTAND

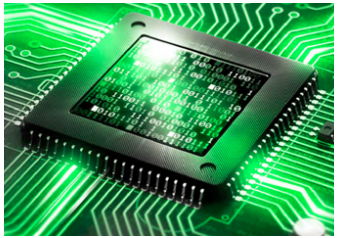
Know you are being hacked
and how, in real time
Monitor > Detect > Analyze.



RESPOND

Mitigate the damage and
immunize the fleet in hours
with software updates
over-the-air

EBs product portfolio for Security



Hardware specific security products

Microcontroller specific software to enable the hardware security features and abstract to the higher level basic software.

Security solutions for applications

Different security software components on the application layer for multiple functions and use-cases.

AUTOSAR basic software

The security AUTOSAR basic software stack enables the application to utilize hardware enhancements and accelerate crypto-graphic calculations.

Security solutions for bootloader

Verification and authen-tication for bootloader software to ensure flawless operation regarding startup, software exchange, and diagnostics.

Software update over-the-air

Solution is ready to update the complete car, multi-ECUs, as well as In-Vehicle Infotainment (IVI) and other performance ECUs. Platform independent onboard OTA components.

Security consulting

Consulting subject-matter experts and generating strategies to handle complex software development projects.

Get in touch!

jochen.olig@elektrobit.com
https://elektrobit.com