Cybersecurity in Mobility Systems

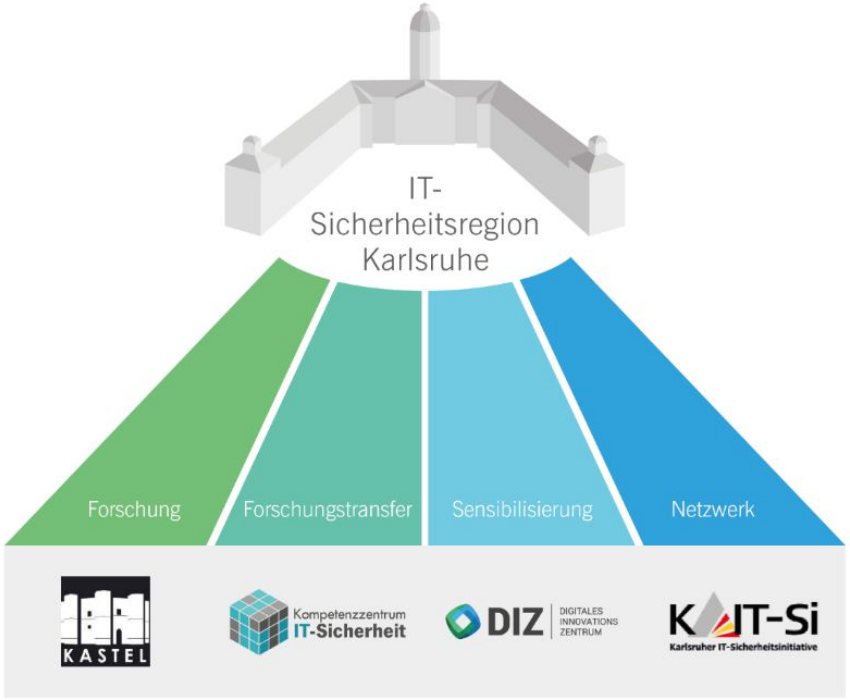
PD Dr.-Ing. Ingmar Baumgart

Competence Center for IT Security @FZI

IT security for SMEs in Baden-Württemberg

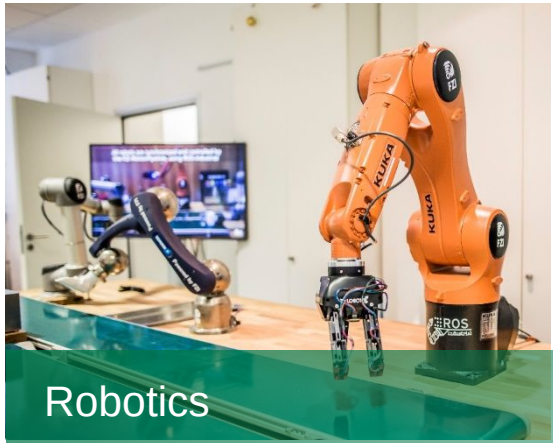
- The Competence Center for IT Security provides a **holistic approach towards secure systems**
  - Fundamental methods and concepts of IT security
  - Knowledge of the application fields
  - Continuous assessment of IT security over the entire product life cycle
- Part of the IT security region Karlsruhe
  - Cooperation of **centers and initiatives** that deal with **IT security** on **all levels**

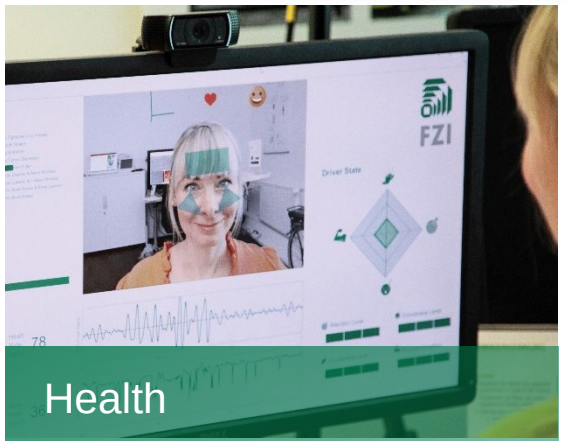
Kompetenzzentrum IT-Sicherheit



Cybersecurity is a requirement for digitalization

The Internet of Things is ubiquitous





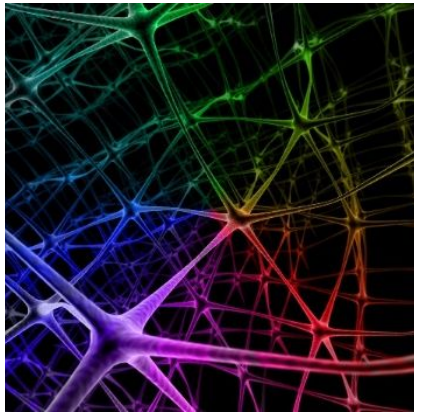
…and introduces major challenges for cybersecurity

Interaction with the environment

Embedded systems with sensors and actuators can threaten people and the environment
(safety and privacy)

Worldwide attack surface

The interconnection of embedded systems via the Internet increases the attack surface enormously



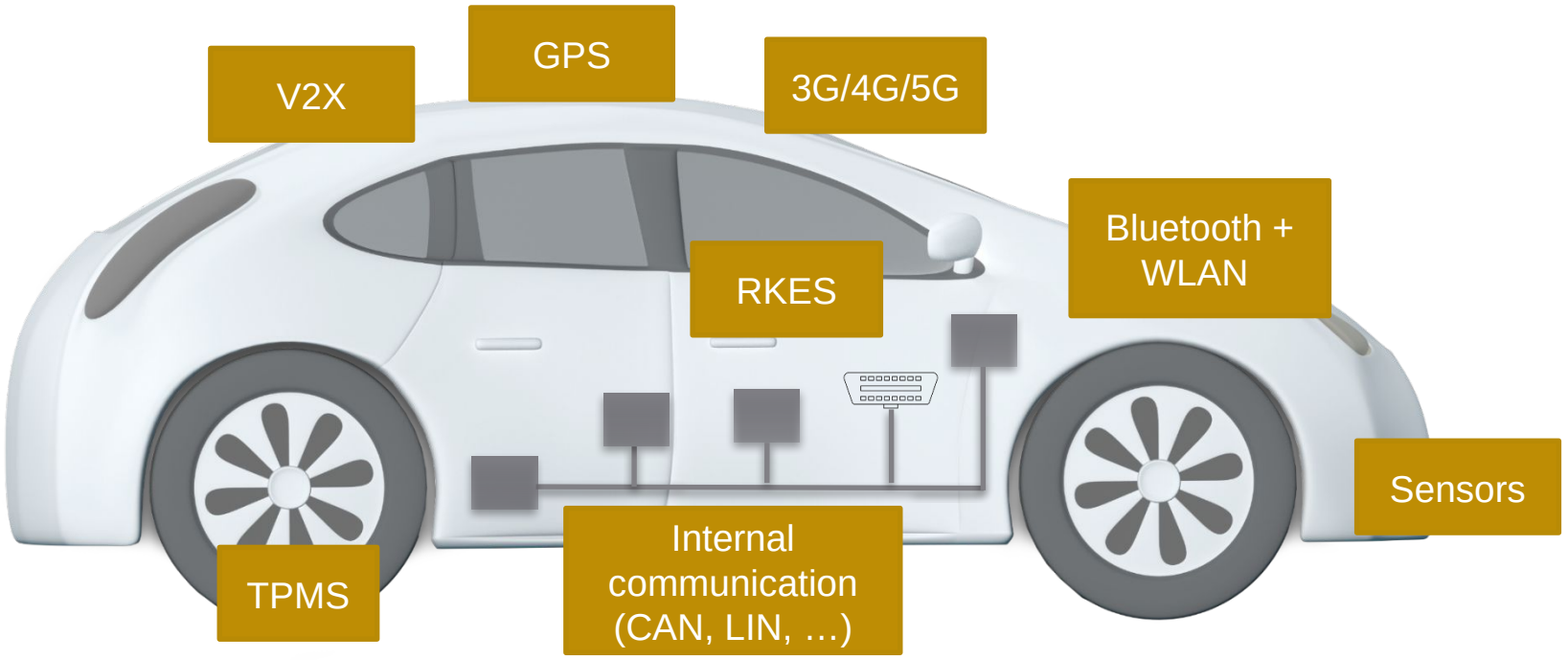
Scalable attacks

Even attackers with limited resources can attack a large number of devices simultaneously

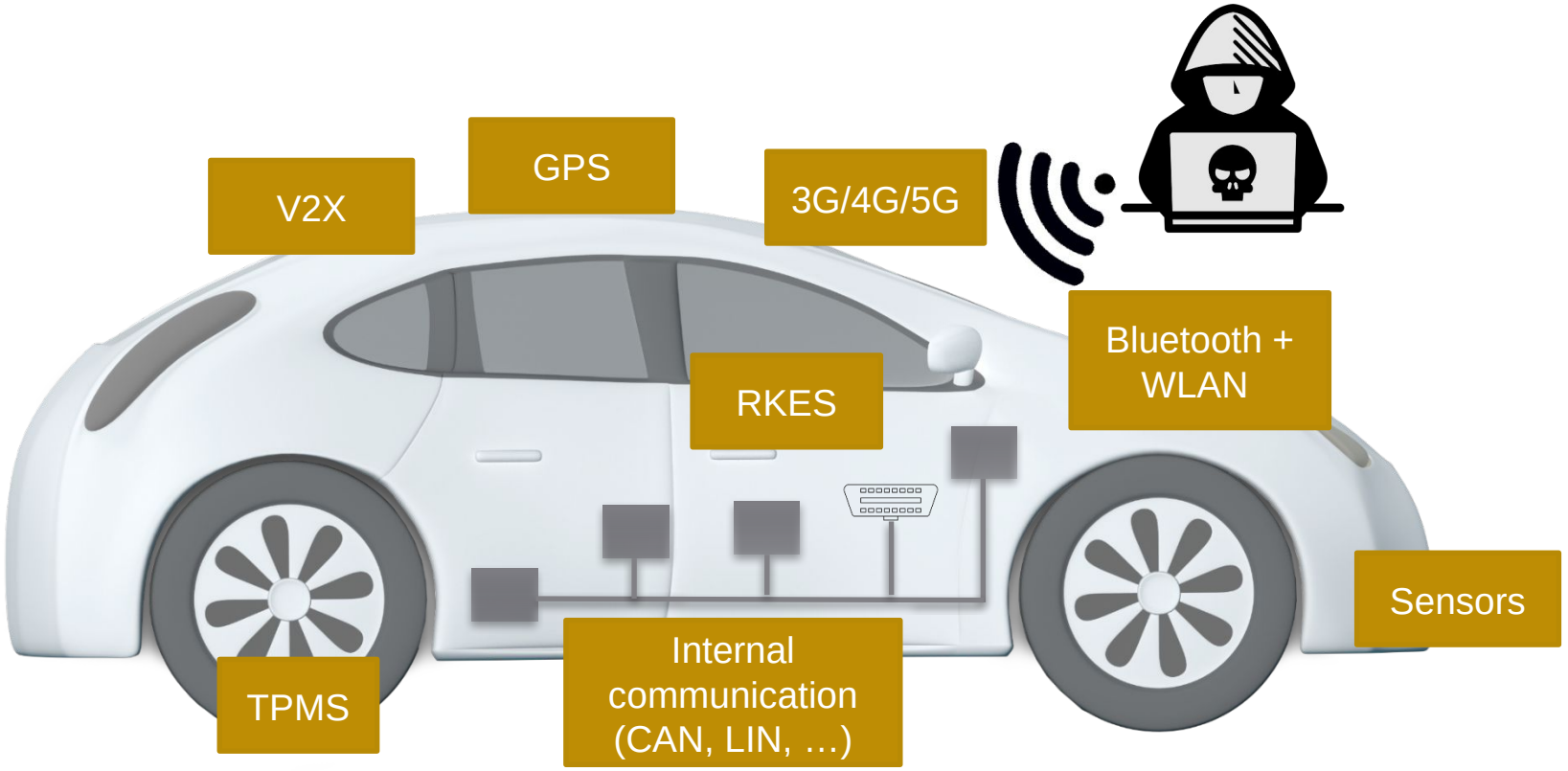
Long product lifetime

In many cases low budget for IT security measures and lifetime updates

Attacks surfaces of a modern vehicle



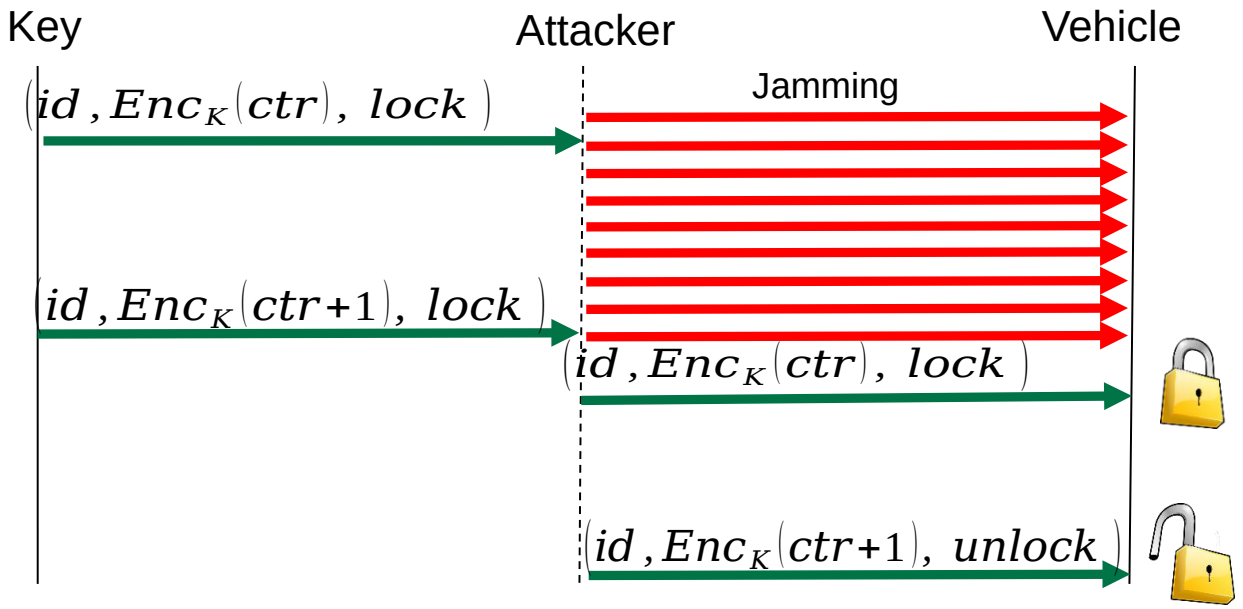
Attacks surfaces of a modern vehicle

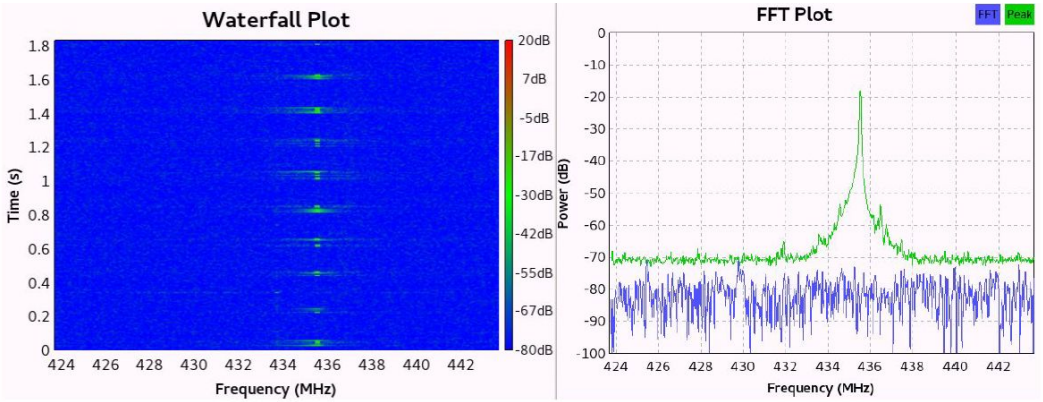


- **Over-the-Air-Updates (OTA) needed to fix vulnerabilities in ECUs**

Example: Security of remote keyless entry systems

- Reverse engineering of proprietary wireless communication protocols using SDRs
- Successful demonstration of Man-in-the-Middle attacks on rolling codes



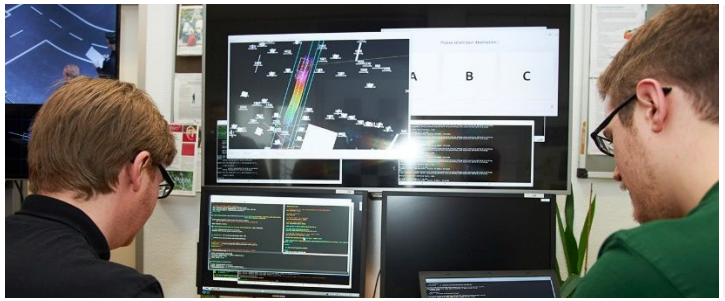


New technologies - opportunities and risks for cybersecurity

New technologies - opportunities and risks

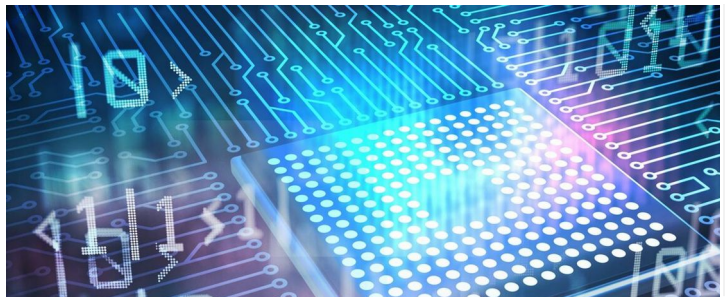
Distributed ledger technologies

Decentralized data storage without central trust anchor



Artificial Intelligence

The use of machine learning creates new avenues of attack ("adversarial machine learning")



Quantum computing

In the future quantum computing could be used to break public key cryptography

In what ways could AI improve IoT security?

Intrusion detection

In many scenarios, machine learning can be used to **detect anomalies (e.g. in network traffic) caused by attacks.**

Malware detection

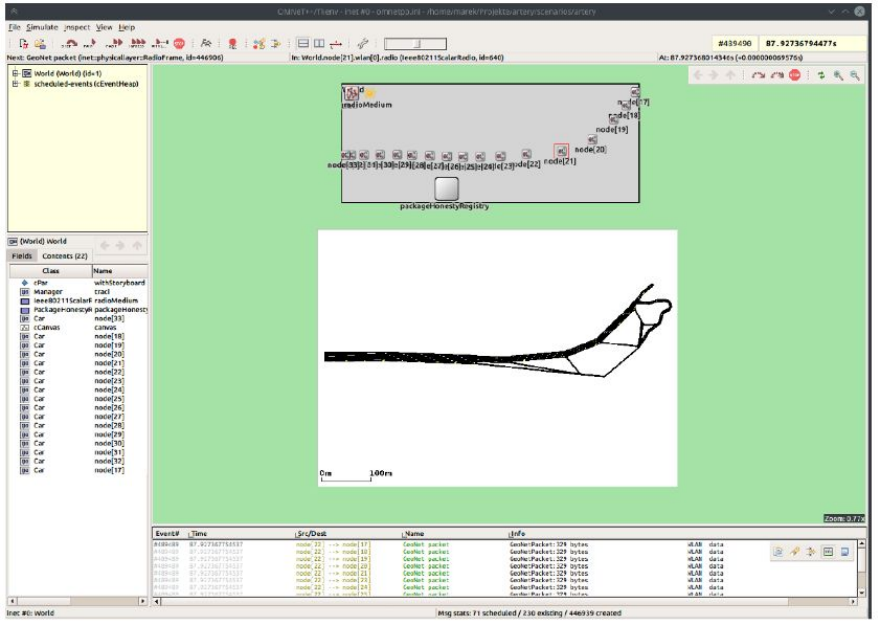
Machine learning can be utilized to **analyze the behavior of executables,** which can be used to prevent the execution of malicious code.

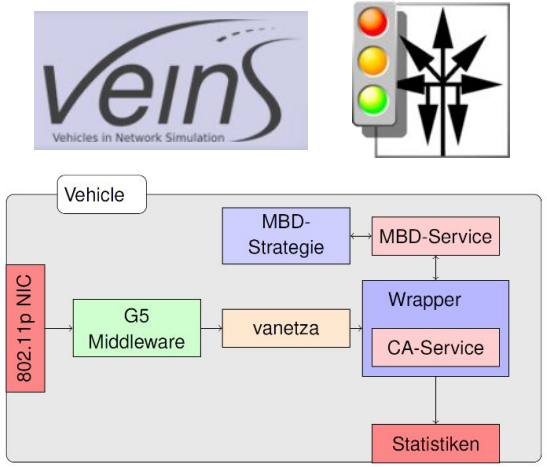
Vulnerability discovery

There a several promising AI-based approaches to **detect vulnerabilities** in **source code** and **binaries**. This could help to reduce costs for security testing of IoT devices in the future.

Research: Intrusion detection systems for V2X

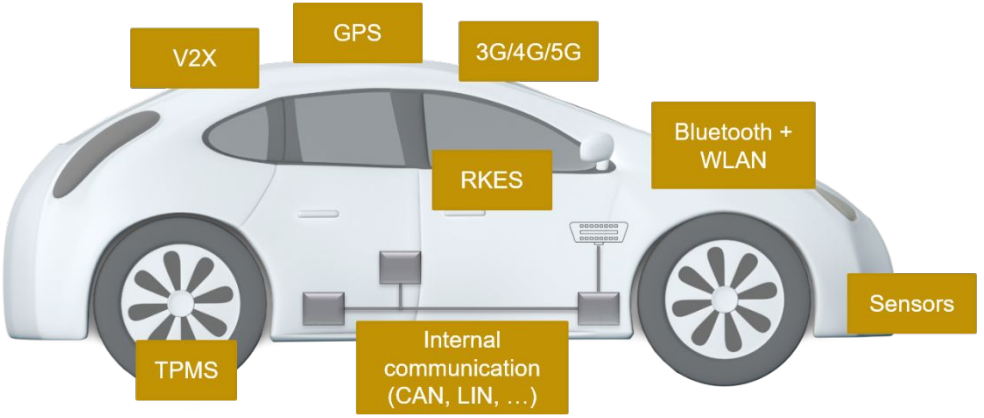
- Evaluation of attacks and intrusion detection systems in realistic scenarios
- Efficient prototyping and evaluation of new IDS approaches
- Simulations based on SUMO and veins





Conclusion

- **Many cybersecurity challenges for mobility systems**
  - Interaction with the environment
  - Worldwide attack surface
  - Scalable attacks
  - Long product lifetime



- Current IoT devices often have **major security vulnerabilities**
- New technologies like **DLT**, **AI** and **quantum computing** introduce new risks, but also offer chances for cybersecurity in future mobility systems

Kompetenzzentrum IT-Sicherheit

Our Research Shapes the Future

FZI Research Center for Information Technology

But...

Attackers make use of AI-based tools to carry out attacks

Legitimate vulnerability detection tools can also be used by attackers to exploit third-party systems.

AI raises new attack surfaces

Machine learning is vulnerable to several attack itself (“adversarial machine learning”). Attackers could use the attacks to e.g. manipulate speech and image recognition in IoT devices.

Common vulnerabilities in IoT devices

Insecure firmware updates

 Authenticated firmware updates (e.g. using TLS)

Insecure remote access

 Limit remote access and utilize network segmentation

Improper use of passwords

 Use alternatives to passwords (e.g. asymmetric cryptography)

Missing authentication

 Proper verification of both client and sender certificates

Bugs in implementation

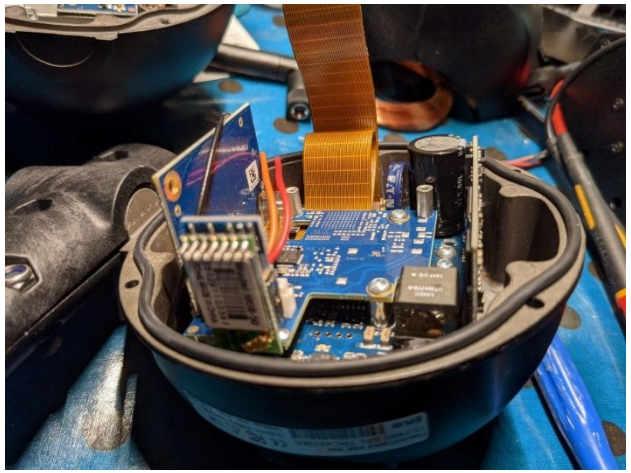
 Code reviews and secure coding process

Wrong use of crypto

 Use of established libraries

Security of V2X components

- Customizable V2X framework „Vanetza“ (CARISMA, Hochschule Ingolstadt) with security extensions for flexible field tests
  - Message signatures / validations
  - Certificate cache and certificate chain validation
  - Interoperability with deployed RSUs



- Security testing of V2X components
  - Hardware attacks (glitching, EM fault injection, JTAG)
  - Fuzzing of network interfaces