Automotive Cybersecurity

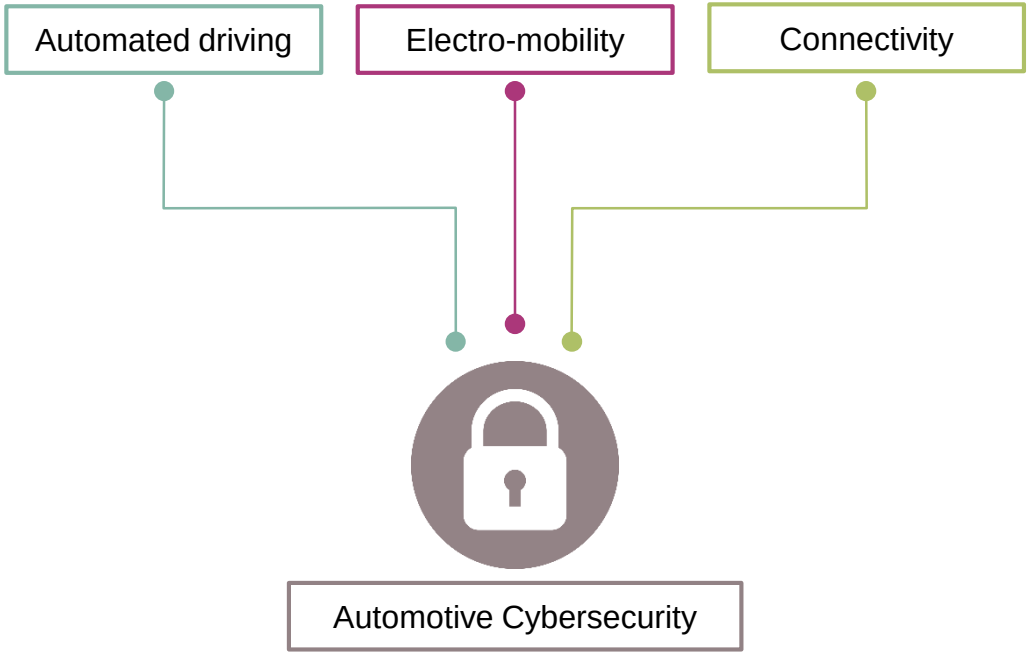
Infineon Automotive Dependability

Quality
Cybersecurity
Functional Safety
Dependable Electronics

Infineon

Cybersecurity is defining the next level of quality for the automotive industry

The Automotive Market is currently shaped by four Megatrends. They are all linked to Automotive Cybersecurity



Infineon is your trusted advisor for a holistic automotive cybersecurity approach

The combined ATV and CSS divisions result in leading-edge products!

Connected car revolution

Every connection in the car is a potential point for an attacker…

Attack scenarios

…and, unfortunately, they seem to have unlimited creativity!

Software — Hardware

Logic attacks	Side channel attacks	Fault injection	Invasive attacks
Protocol fuzzing, jamming, replay	SPA, DPA, spectre, meltdown	Spiking, radiation, light attacks, clock manipulation, DFA	FIB manipulation, microprobing

What countermeasures can be implemented?

Attack scenarios

…What countermeasures can be implemented?

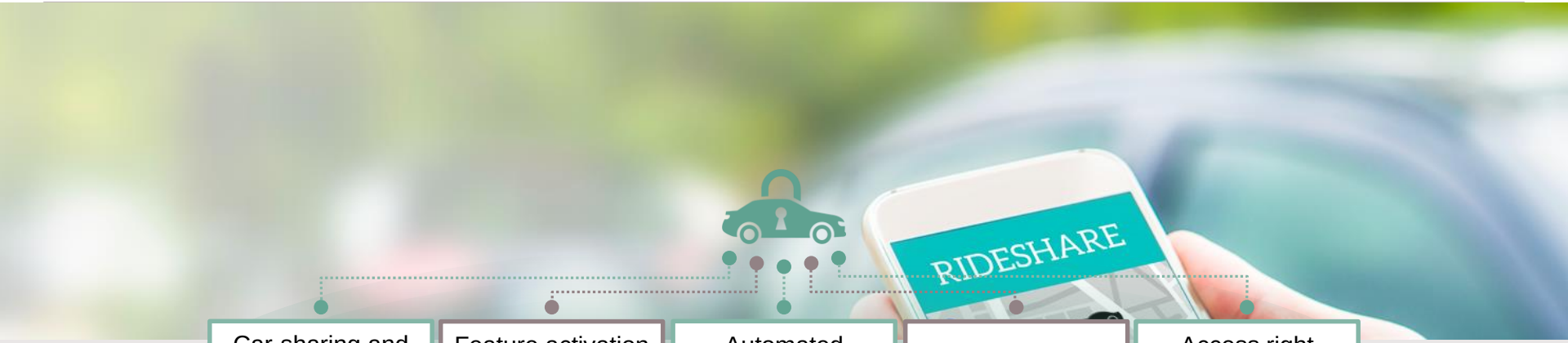
Software

Hardware

Logic attacks	Side channel attacks	Fault injection	Invasive attacks
PKI, digital signatures, encryption, CMAC, blockchain, MISRA C-CERT coding guidelines	Run-time invariant SW implementation, randomization in HW and SW, dual-rail HW implementation, encrypted computation	Double computation, all safety HW measures	Tamper protection, implanted ROM, full-custom design

Security always consists of a combination of hardware and software

But not everything is bad news. Security is the enabler for new business models



Car-sharing and ride-sharing

Feature activation (on demand)

Automated driving

Payment

Access right delegation

Which assets need to be protected?

Security certificates and cryptographic keys

Embedded code and data (IP protection)

Personal user data

We offer the most scalable automotive cybersecurity portfolio, meeting the right level of security

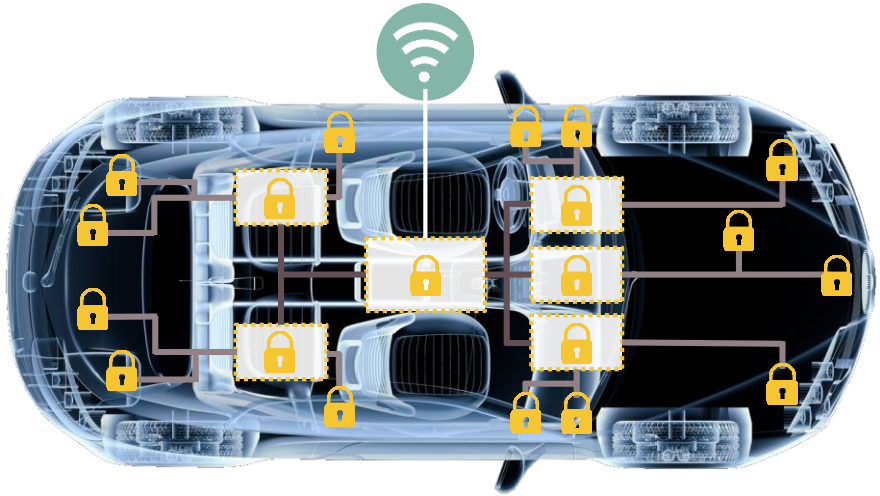
Infineon offers the most scalable automotive cybersecurity product portfolio, meeting the RIGHT level of security for your application!

Security

Discrete security controller	Hardware trust anchor + software + tamper resistance e.g. **Infineon OPTIGA™ TPM & SLS37 V2X HSM**
Integrated HSM*	Separated and protected run-time environment E.g. **Infineon AURIX™ & TRAVEO II HSM**
Trusted execution environment	Separation of "secure" and "normal" world in one CPU
Host	Pure software protection

*HSM = Hardware Security Module

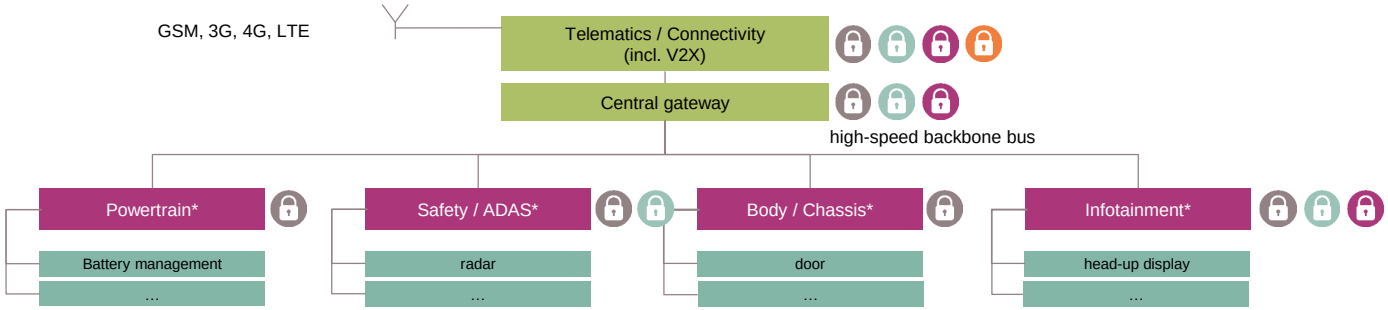
Principles of cybersecurity



Different Layers of Security are required in future Car Architectures

- Secure platform
- Secure onboard communication
- Secure network separation
- Secure external communication

Infineon's automotive security offering
A scalable portfolio for dedicated applications



AURIX™ family TRAVEO™ II family	SEMPER™ SECURE Flash	OPTIGA™ TPM	eSIM SLI 37
On board security across all domains › HW Security Module (HSM or SHE) (AURIX™ TC2x & TC3x) › Cyber Security Realtime Module & Satelites (AURIX™ TC4x) › Full EVITA compliant (AURIX™ TC3x) › Ethernet security features (AURIX™) › Unique chip individual keys › Security SW lib › Safety Features against fault attacks (up to ASIL-D) › Automotive qualified with zero ppm automotive quality	**Hardware root-of-trust for Application processors** › ASPICE level 2 firmware › Secured storage regions › Hardware crypto engine › Ephemeral session keys › Mutual device authentication › Automotive qualified › ASIL-B compliant	**Authentication, secured key store, on-chip key generation & management** › Tamper resistant hardware › TPM2.0 SW compliant › Initial keys and certificates › Automotive qualified Hardware + Software certified acc. to Common Criteria	**Enabling cellular connectivity** › Tamper resistant hardware › eSIM SW functionality › Initial keys and certificates › Automotive qualified › Hardware certified acc. to Common Criteria
Integrated HSM	Discrete Hardware Security		

A dependable communication in an interconnected system has security as an integral part

No Safety without security

- Security is a mandatory precondition for Safety
- Safety is the most important asset to be protected
- A dependable architecture is secure and safe

Security is an architecture property

- A secure EE-architecture is always built around a certified root-of-trust
- Hardware/Software co-design is key for a strong protection scheme
  - Appropriate security is required on all layers of the EE-architecture

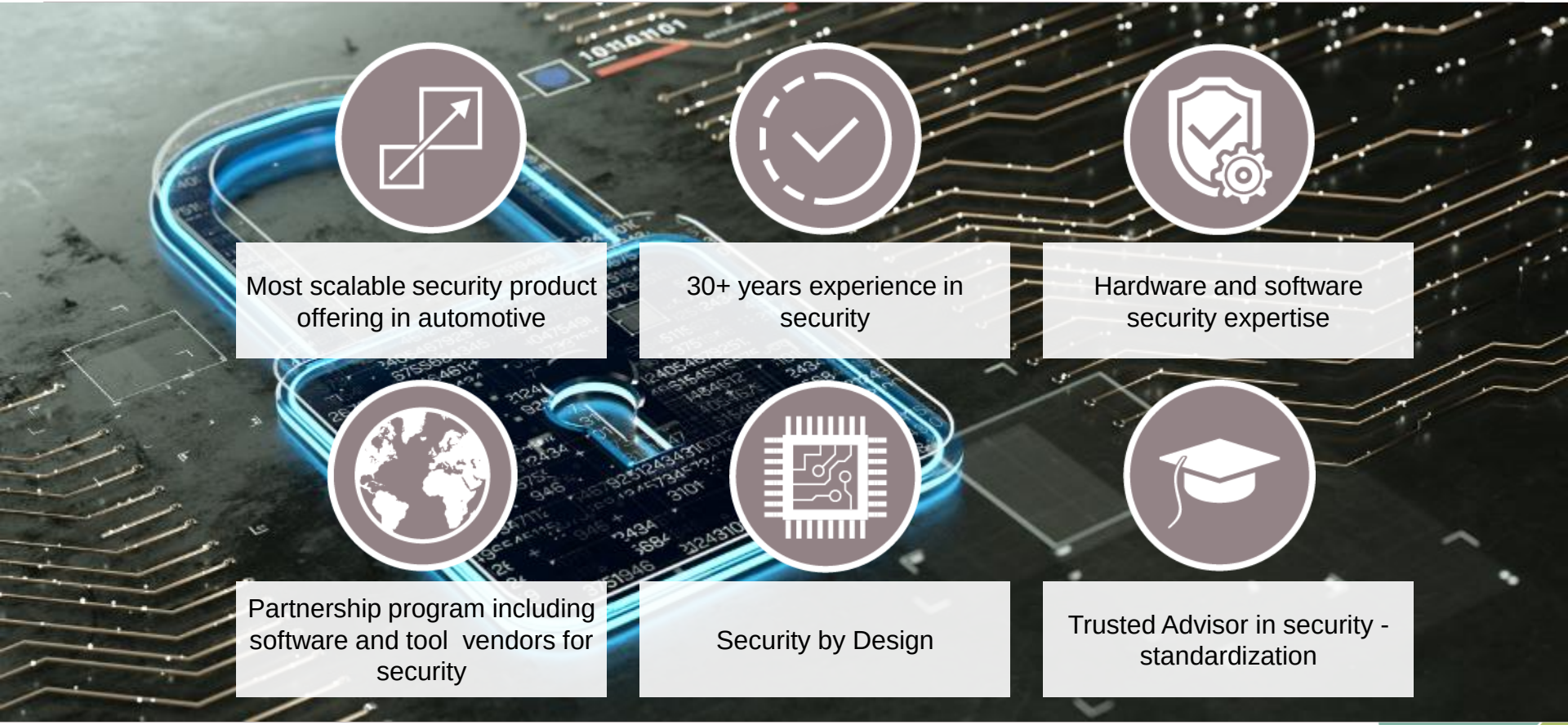
Security is a moving target

- Security erodes over time
- Always be ahead of the attacker's capabilities
- Crypto-agility is a must – the right hardware is an enabler for this

Security needs cooperation

- Security by obscurity is not sustainable
- Security standards allow transparent risk management over the complete lifecycle
- Incident management processes across the whole supply chain have to be established

Infineon – Automotive CyberSecurity Leadership beyond Hardware



Most scalable security product offering in automotive

30+ years experience in security

Hardware and software security expertise

Partnership program including software and tool vendors for security

Security by Design

Trusted Advisor in security - standardization

Part of your life. Part of tomorrow.

For more information click on the respective image below

Infineon Automotive Dependability

Quality
Cybersecurity
Functional Safety
Dependable Electronics

Dependable Electronics