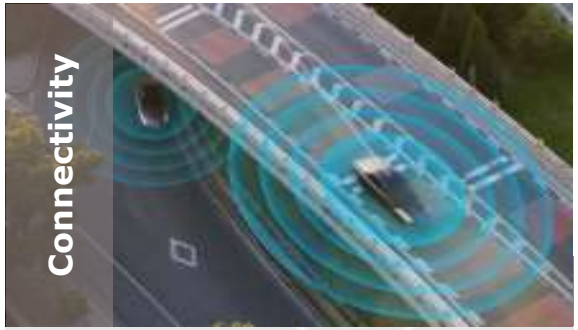
TRUSTED DRIVING

Dr. Huang XianMing
18th October 2018

Megatrends shaping the automotive market; significantly increasing semi content per car

Enabling safety towards Vision Zero

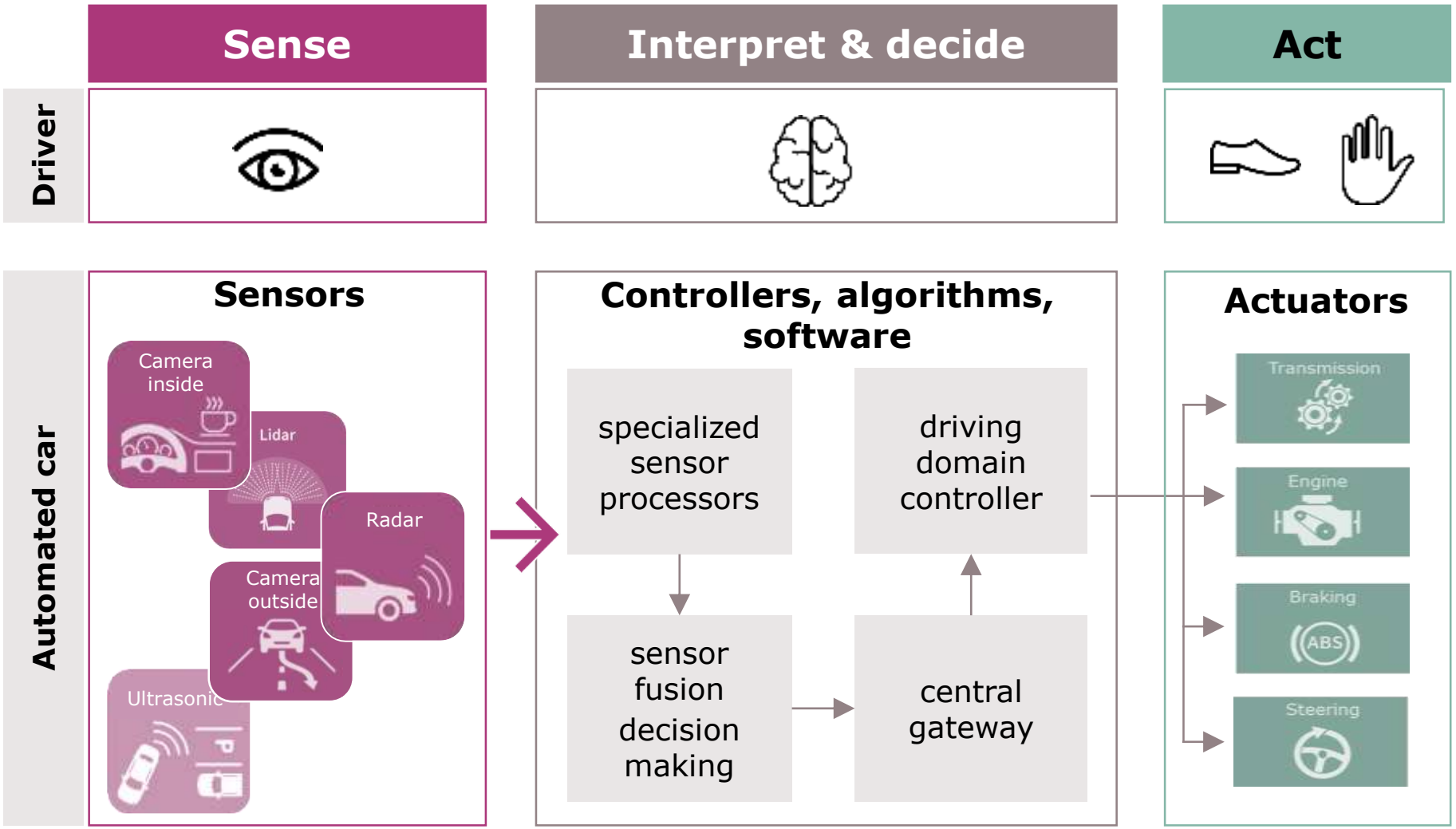
Enabling CO_2 reduction



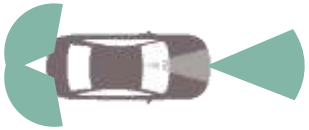
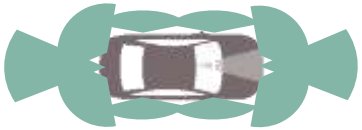
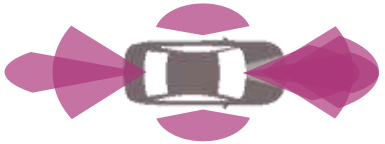
Enabling the communication of cars

Enabling security in connected cars

For Automated Driving more compute power but also a higher security and safety is needed



More sensors required for any next level of automation will lead to sensor cocoon in L4/5

	Level of automation		
	Level 2	Level 3	Level 4/5
Application*	Automatic emergency brake/ forward collision warning		
	Parking assist		Valet parking
	Lane keep assist	Highway assist	Highway and urban chauffeur
Radar # of modules**	 ≥ 3	 ≥ 6	 ≥ 10
Camera # of modules**	 ≥ 1	 ≥ 4	 ≥ 8
Lidar # of modules**	0	 ≤ 1	 ≥ 1
Others	Ultrasonic	Ultrasonic Interior camera	Ultrasonic Interior camera V2X

* Source: VDA (German Association of the Automotive Industry); Society of Automotive Engineers
** Market assumption

Outstanding characteristics make AURIX™ first-choice µC in the AD platform market

AURIX™ is the market reference as host controller in central computing platforms complementing CPU/GPU to make central computer robust and fail operational

Drive PX2

NVIDIA

Go™ Automated Driving Platform with AURIX™

TTTech MotionWise

Elektrobit

EB robinos

Baidu 百度

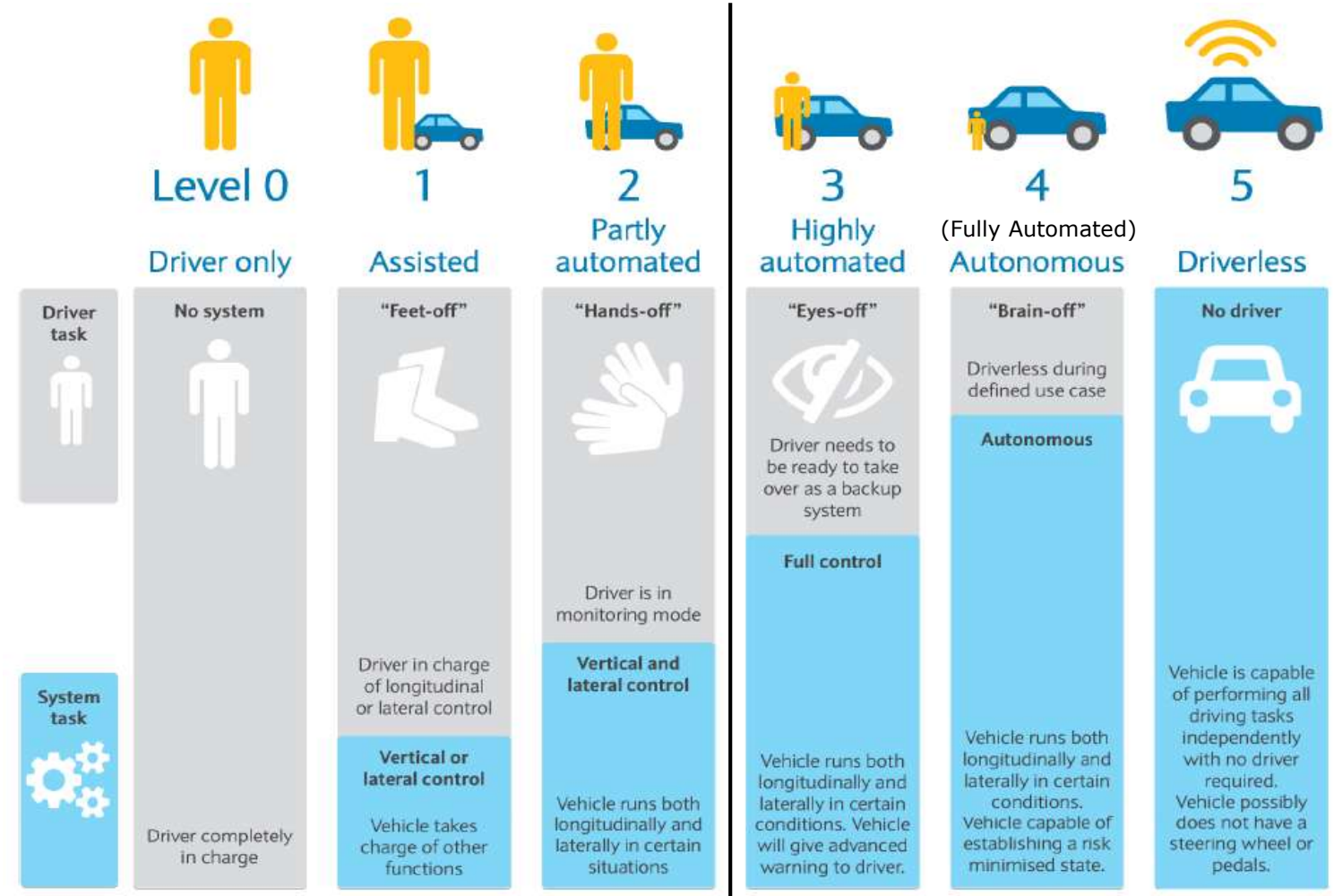
Apollo 2.0 Self Driving Platform

AURIX™

- Safety host monitoring the operation of the data fusion ECU enables ISO 26262 ASIL-D
- Safe and secure gateway to the vehicle network
- Fallback operation in case of a GPU/CPU fail
- Safe communication to actuator control units

- Awareness for safety and security aspects of AD is increasing rapidly
- Infineon is cooperating with the leading AD platform providers

Level 0 – Level 5: SINGLE definition across the globe: NHTSA = VDA = SAE



Source: Barclays Research

ADAS

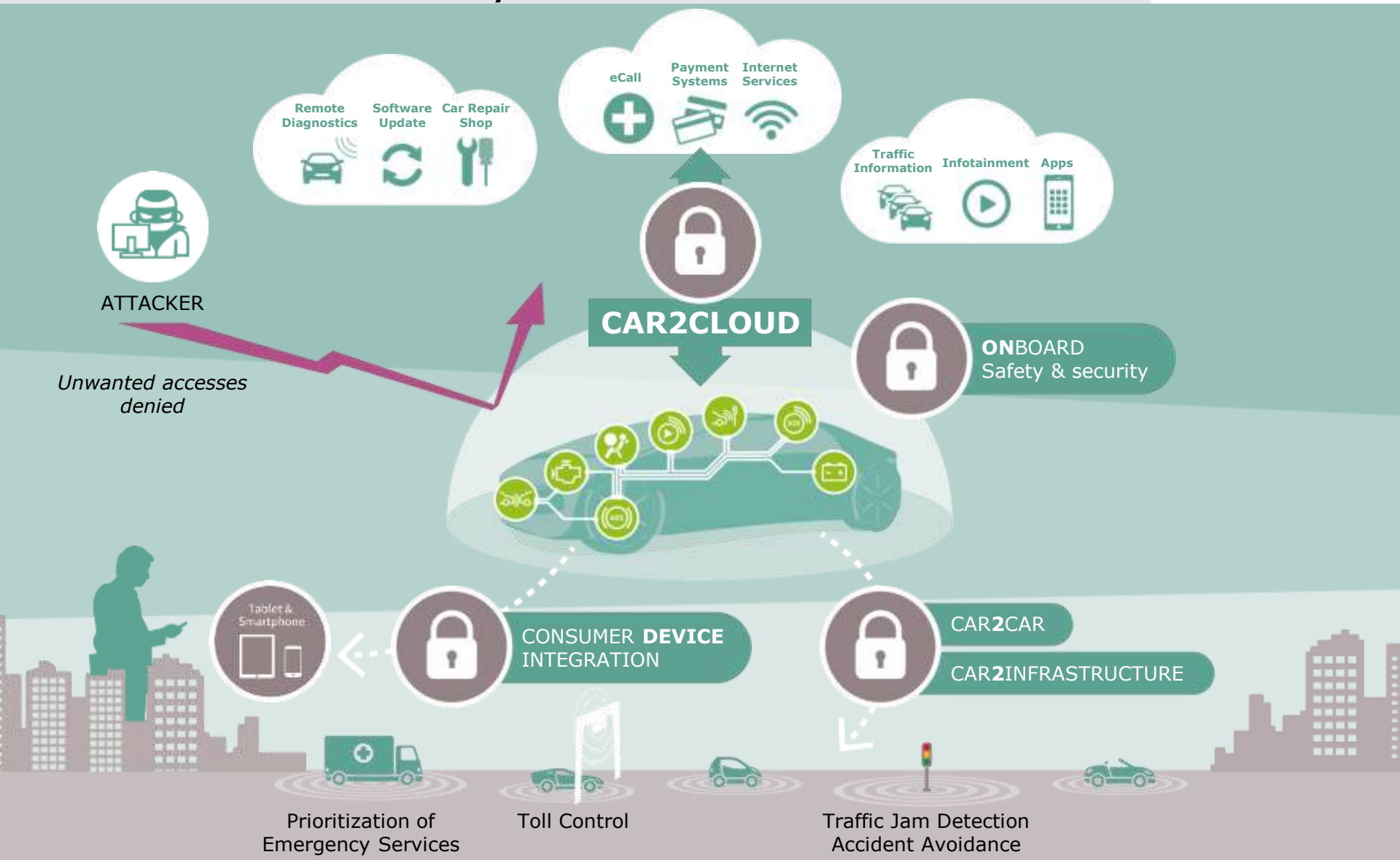
Advanced Driver Assistance Systems

AD

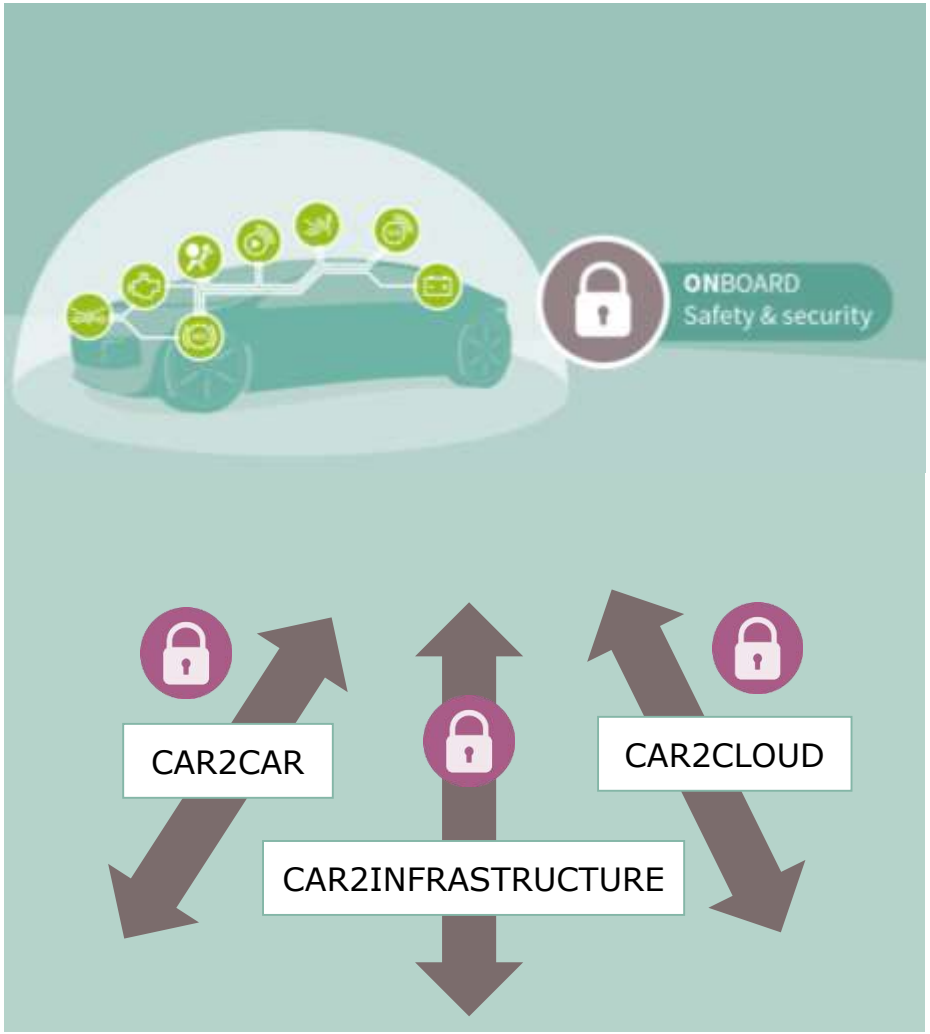
Automated Driving, Fail Operation

Amendments of current regulations are necessary (e.g. Vienna StVO, ECE-R79)

Automotive Security



The importance of trust anchors for Automotive Security



Integrated on MCU (HSM)

- Onboard security
- Protected com. & debug interfaces
- High-speed / real-time critical tasks

Discrete Security Controller

- Protected external communication
- Certified hardware security
- Protecting critical keys & certificates

The leading partner for best-in-class Automotive Security IC solutions

Automotive Customers

Standardization Bodies

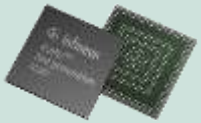
System Know-How

- Tight customer relationship
- Active participation in the decisive standardization bodies and industrial consortia
- System know-how and application understanding

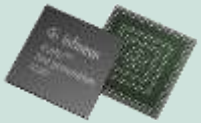
Automotive Cybersecurity Portfolio

AURIX™ 1st & 2nd Gen	SLI 76 SLI 97	OPTIGA™ TPM SLI 9670

Infineon's automotive trust anchor portfolio

	AURIX™ 1st & 2nd Gen	**eSIM IC** SLI 76/97	**V2X IC** SLI 97	**OPTIGA™ TPM** SLI 9670
				
Product type	Multipurpose MCUs for safety apps. (ASIL-D) with embedded Hardware Security Module (**integrated HSM**)	Discrete security hardware (**external HSM**)		
		Cellular connectivity	Security IC for V2X support	Ready-to-use trust anchor: Standardized turnkey solution
Security level	Separate Crypto-Core and e-Flash, read-out protection, limited hardware resistance	Hardware tamper resistant & security certified according to highest industry standards		
		Certification of HW only	Certification of HW only	Certification of HW **+ FW**
Quality level	Fully Automotive (AEC Q-100 Grade 0+) incl. zero defect efforts, DFR, robust materials	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	Programmable (Crypto Lib avail.)	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + **secure coding**
ECU individual personalization	Unique chip identifier	Initial keys and certificates (on request)	Initial keys and certificates (on request)	Initial key and certificate (on request)

Infineon's automotive trust anchor portfolio

	AURIX™ 1st & 2nd Gen	**eSIM IC** SLI 76/97	**V2X IC** SLI 97	**OPTIGA™ TPM** SLI 9670
				
Product type	Multipurpose MCUs for safety apps. (ASIL-D) with embedded Hardware Security Module (**integrated HSM**)	Discrete security hardware (**external HSM**)		
		Cellular connectivity	Security IC for V2X support	Ready-to-use trust anchor: Standardized turnkey solution
Security level	Separate Crypto-Core and e-Flash, read-out protection, limited hardware resistance	Hardware tamper resistant & security certified according to highest industry standards		
		Certification of HW only	Certification of HW only	Certification of HW **+ FW**
Quality level	Fully Automotive (AEC Q-100 Grade 0+) incl. zero defect efforts, DFR, robust materials	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	Programmable (Crypto Lib avail.)	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + **secure coding**
ECU individual personalization	Unique chip identifier	Initial keys and certificates (on request)	Initial keys and certificates (on request)	Initial key and certificate (on request)

HSM Within EVITA Context Mapping on IFX Products

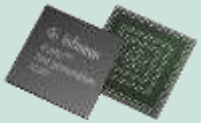
EVITA[1] Classification within automotive Hardware Security Module	HIS / Infineon	EVITA	EVITA / Infineon	EVITA / Infineon
		Light EVITA HSM	**Medium EVITA HSM**	**Full EVITA HSM**
HSM secure internal RAM	key RAM only	optional	✓	✓
HSM private NVM (e.g. Key Storage, Secure Data)	key storage only	optional	✓	✓
symmetric HW Crypto Engine (e.g. 128-bit AES)	✓	✓	✓	✓
Asymmetric HW Crypto Engine (e.g. ECC256)	—	—	—	✓
HW Hash Engine (e.g. SHA1, SHA2, ...)	—	—	—	✓
RNG (Random Number Generator)	TRNG ✓	PRNG (with ext. seed)	TRNG ✓	TRNG ✓
Secure CPU	State Machine (HIS compliant API)	—	✓	✓
Secure Application Use Cases	Immobilizing, Anti-Theft Secure Boot, Key Storage	Secure Sensors Secure Satellite ECU	Powertrain , Braking, Chassis ECUs (various)	Car2Car / Car2x Communication
IFX Implementations	**AUDO MAX - SHE** (TC1791/93/98)	not applicable for µC	**AURIX Performance HSM** (TC29x / TC27x) **AURIX Efficiency HSM** (TC23x)	**TC3xx (TC3xx)**

(1) EU-funded project (2008-2011) on secure automotive onboard networks - www.evita-project.org
(2) Secure Hardware Extension - SHE, Standard by HIS ("Hersteller Initiative Software" by German OEMs)

AURIX™ covers majority of use cases

AURIX™ use cases	Powertrain	Chassis / Safety / ADAS / AD	Body / advanced connectivity
		 	
ICE	engine management	domain control	chassis suspension	vehicle stability control	advanced body control module	over-the-air update
ICE	transmission	power steering	electric parking brake	airbag and safety	connected gateway	online control module
ICE	starter generator	77 GHz radar	24 GHz radar	advanced lighting		
xEVs	BEVs HEVs, PHEVs	DC-DC converter	driver monitoring	sensor fusion	vision safe host controller	infrastructure controller for V2V/V2X
xEVs	onboard charger	battery management				
growth driver	› unit production › xEV penetration	› ADAS/AD penetration › evolution from L0 towards L5	› comfort penetration › connectivity

Infineon's automotive trust anchor portfolio

	AURIX™ 1st & 2nd Gen	**eSIM IC** SLI 76/97	**V2X IC** SLI 97	**OPTIGA™ TPM** SLI 9670
				
Product type	Multipurpose MCUs for safety apps. (ASIL-D) with embedded Hardware Security Module (**integrated HSM**)	Discrete security hardware (**external HSM**)		
		Cellular connectivity	Security IC for V2X support	Ready-to-use trust anchor: Standardized turnkey solution
Security level	Separate Crypto-Core and e-Flash, read-out protection, limited hardware resistance	Hardware tamper resistant & security certified according to highest industry standards		
		Certification of HW only	Certification of HW only	Certification of HW **+ FW**
Quality level	Fully Automotive (AEC Q-100 Grade 0+) incl. zero defect efforts, DFR, robust materials	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	Programmable (Crypto Lib avail.)	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + **secure coding**
ECU individual personalization	Unique chip identifier	Initial keys and certificates (on request)	Initial keys and certificates (on request)	Initial key and certificate (on request)

Infineon in the eSIM market since 2008

2007	Definition in collaboration with Axalto
2008	Standardization with ETSI
2009	Launch of first automotive project with GTO – DTAG – Harman Becker - IFX
2012	Introduction of SLI quality brand (AEC-Q100 + PPAP + Ext. Control)
2014	Launch of SLI 97 Platform

Delivering field-proven high quality since 2008!

High volume deliveries and proven track record since then!

Infineon supplying IC for the eSIM of the telematics and infotainment box since 2009

SLI 97 NEW

32-bit ARM® SC300™
600KB, 800KB and 1MB NVM
32 KB RAM
3DES, AES, RSA
CC EAL 5+ High

SLI 76

16-bit
Up to 512 KB NVM
8 KB RAM
3DES, AES (SW)

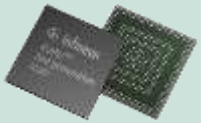
-40 to +105 °C
17 years lifetime

AEC Qualified

Multiple Subscription - eUICC Spec

Single Subscription

Infineon's automotive trust anchor portfolio

	AURIX™ 1st & 2nd Gen	**eSIM** SLI 76/97	**V2X IC** SLI 97	**OPTIGA™ TPM** SLI 9670
				
Product type	Multipurpose MCUs for safety apps. (ASIL-D) with embedded Hardware Security Module (**integrated HSM**)	Discrete security hardware (**external HSM**)		
		Cellular connectivity	Security IC for V2X support	Ready-to-use trust anchor: Standardized turnkey solution
Security level	Separate Crypto-Core and e-Flash, read-out protection, limited hardware resistance	Hardware tamper resistant & security certified according to highest industry standards		
		Certification of HW only	Certification of HW only	Certification of HW **+ FW**
Quality level	Fully Automotive (AEC Q-100 Grade 0+) incl. zero defect efforts, DFR, robust materials	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	Programmable (Crypto Lib avail.)	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + **secure coding**
ECU individual personalization	Unique chip identifier	Initial keys and certificates (on request)	Initial keys and certificates (on request)	Initial key and certificate (on request)

“Vehicle-to-X” communication Security partitioning

Security Drivers

1. Network Integrity
2. Privacy

Incoming Messages

Outgoing Messages

Pseudonymous Certificates

Verification

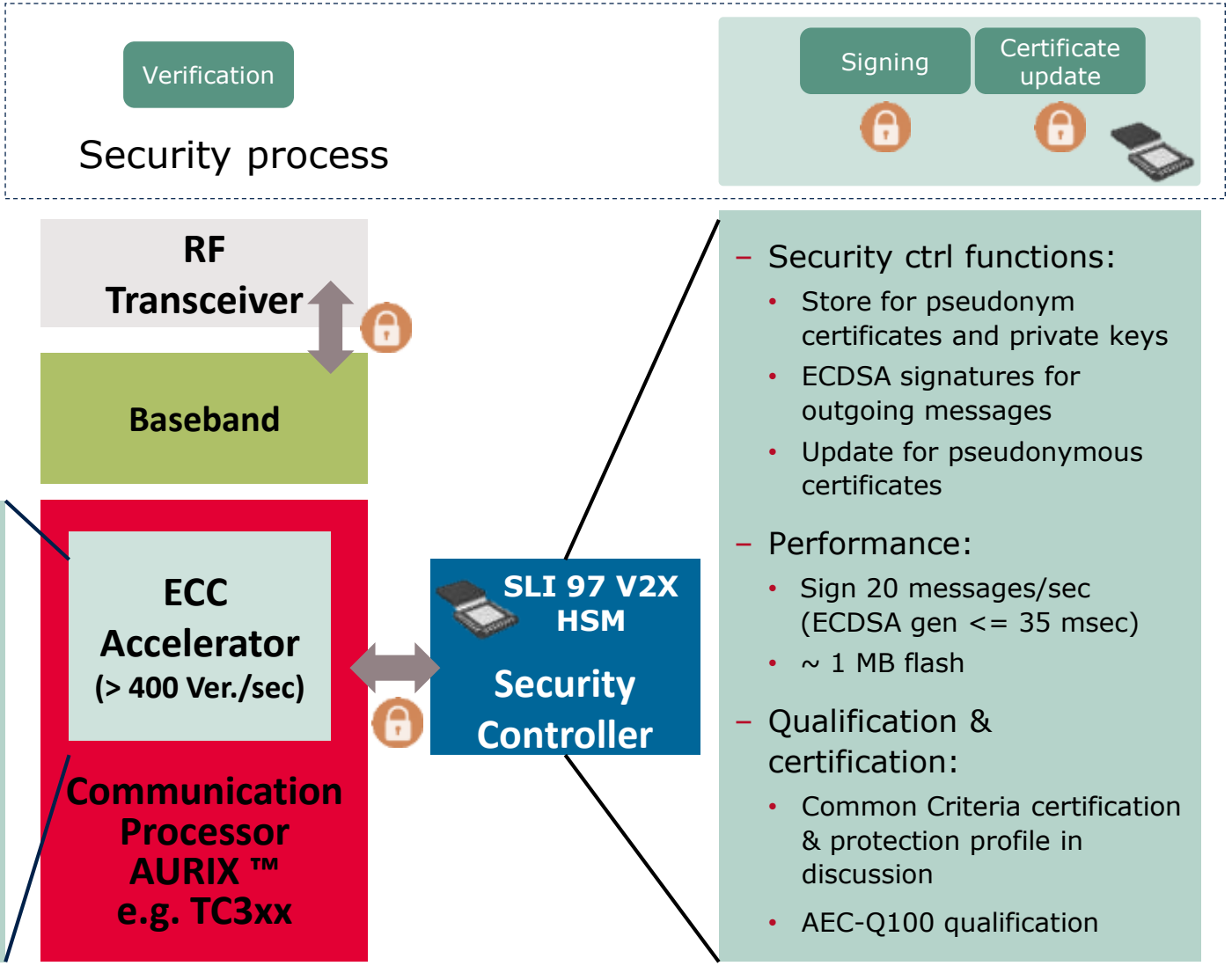
Signing

Certificate Updates

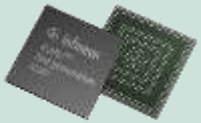
Security Engine

SLI 97 V2X

Architecture and security partitioning



Infineon's automotive trust anchor portfolio

	AURIX™ 1st & 2nd Gen	**eSIM IC** SLI 76/97	**V2X IC** SLI 97	**OPTIGA™ TPM** SLI 9670
				
Product type	Multipurpose MCUs for safety apps. (ASIL-D) with embedded Hardware Security Module (**integrated HSM**)	Discrete security hardware (**external HSM**)		
		Cellular connectivity	Security IC for V2X support	Ready-to-use trust anchor: Standardized turnkey solution
Security level	Separate Crypto-Core and e-Flash, read-out protection, limited hardware resistance	Hardware tamper resistant & security certified according to highest industry standards		
		Certification of HW only	Certification of HW only	Certification of HW **+ FW**
Quality level	Fully Automotive (AEC Q-100 Grade 0+) incl. zero defect efforts, DFR, robust materials	Automotive qualified (AEC Q-100 Grade 2), plus Burn-In, extended process control, tighter process control limits. Due to high security design reduced analyzability and testability.		
Software	Programmable (Crypto Lib avail.)	eSIM standard functions	Programmable (Crypto Lib avail.)	TPM 2.0 standard + **secure coding**
ECU individual personalization	Unique chip identifier	Initial keys and certificates (on request)	Initial keys and certificates (on request)	Initial key and certificate (on request)

OPTIGA™ TPM as Trust Anchor – What is this?

The TPM is a **secure key storage** with **additional security functions**

SW

- Tamper resistance security µC
- Rich set of dedicated HW security features

- IFX own SW
- Firmware + applications (see page 20)
- Secure coded

- Sensitive root key/ certificate

➔ Developed, produced, programmed and personalized in security certified and audited processes

➔ **Common Criteria security certification for the complete security solution**

TPM Security Toolbox (Turnkey Solution)

Authentication

Secure Updates

Boot Protection
Platform Integrity

Key Generation
and Management

Stored Data
Protection

Secure
Communications

ECDH Key Exchange

Securely establish shared symmetric key

PKI

Structured method to handle Public Keys

Certificates

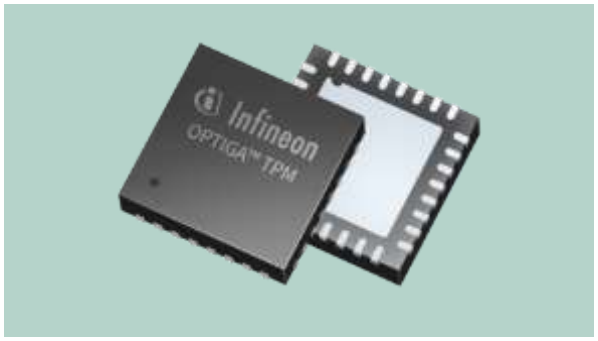
Protect integrity & authenticity of info

Symmetric Encryption	Asymmetric Encryption	Hash Algorithm
Fast Easily Implemented	Secure Key Flexibility	Space Efficient One-way

Summary

Connected cars offer cost saving potentials, convenience gains and new business opportunities. Trust anchors are indispensable in the context

Infineon investigates solutions to provide security by an interplay of AURIX™ and OPTIGA™ TPM



Thereby, Infineon’s scalable portfolio of hardware trust anchors can achieve appropriate security in a cost efficient manner

- 自动驾驶时代一定会到来
- 产业协作，循序渐进