Heterogeneous computing to enable highest level of safety

Ramanujan Venkatadri
Automotive Innovation Center, Infineon Technologies

Table of contents

Table of contents

Challenges with developing autonomous, electric and connected Vehicle

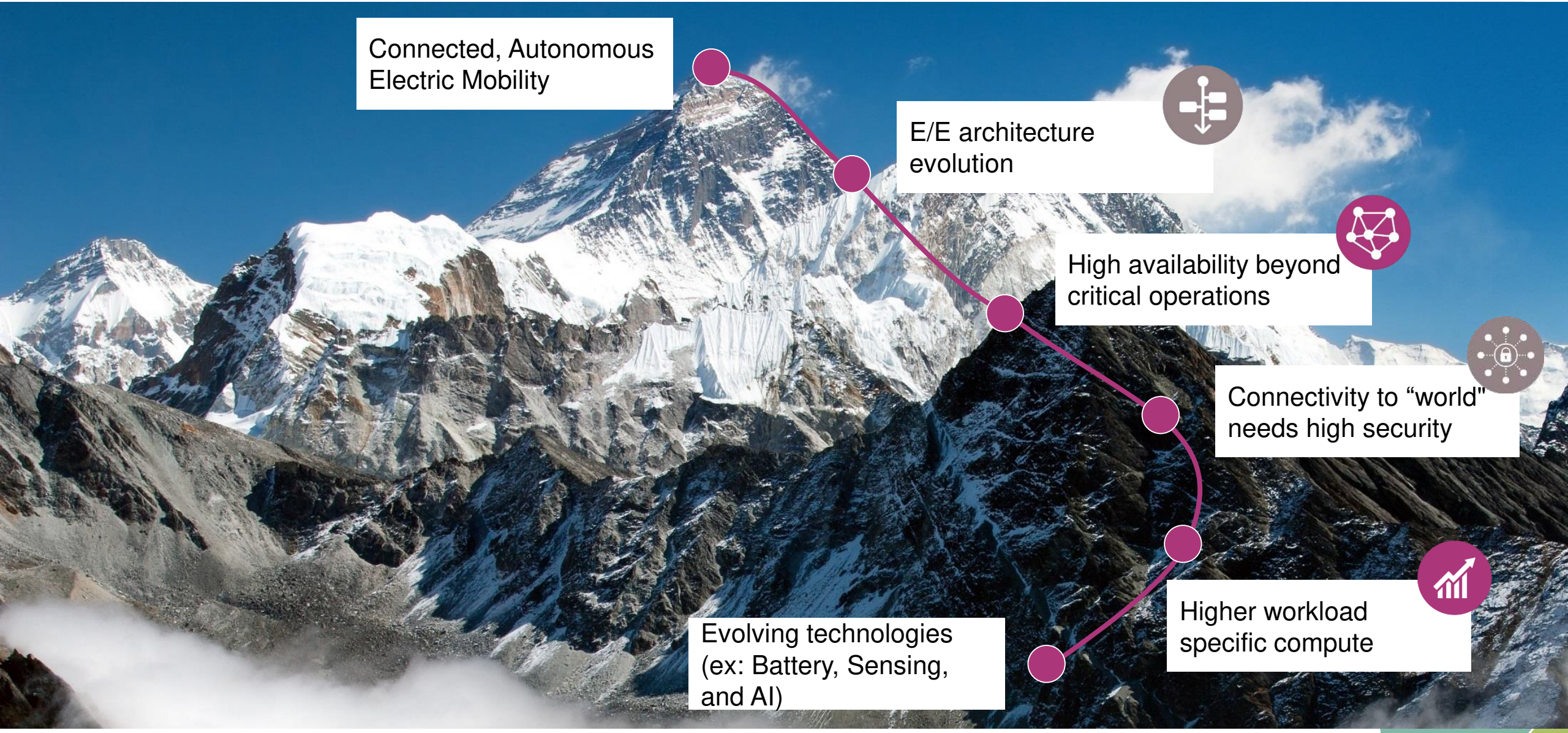
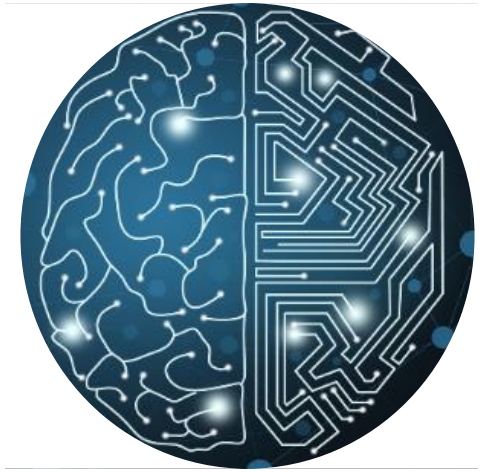
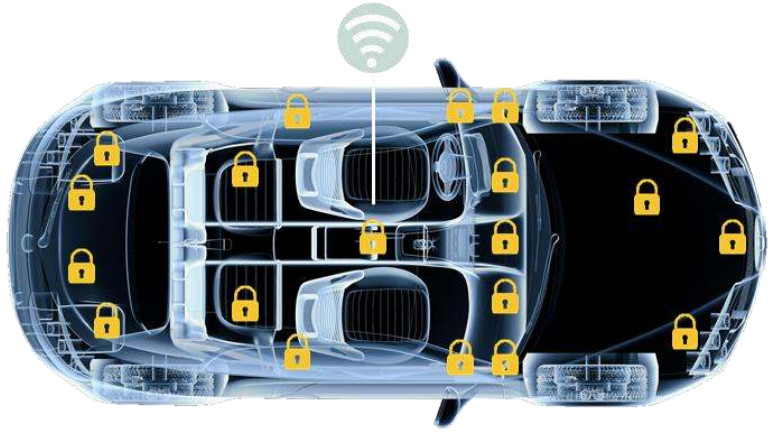


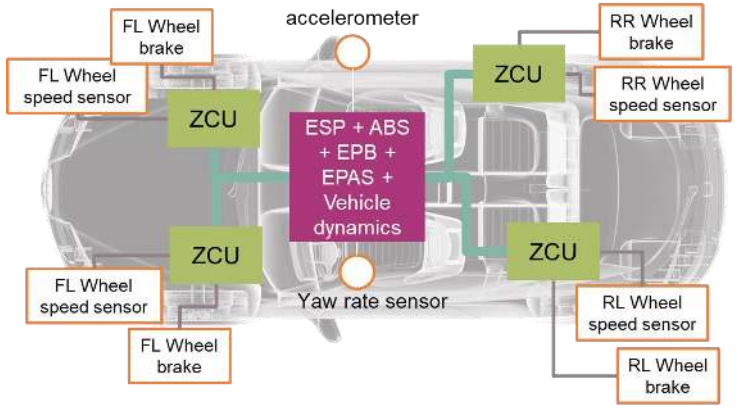
Table of contents

Increase in demand for workload specific compute

1. Artificial Intelligence & sensor specific workload accelerators
2. Faster security accelerators for authenticity & Integrity
3. Higher connectivity interfaces with low latency data processing







- Machine learning
- Sensor processing
- Security
- Faster data processing

Table of contents

The connected mobility : How to secure the future vehicle?

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

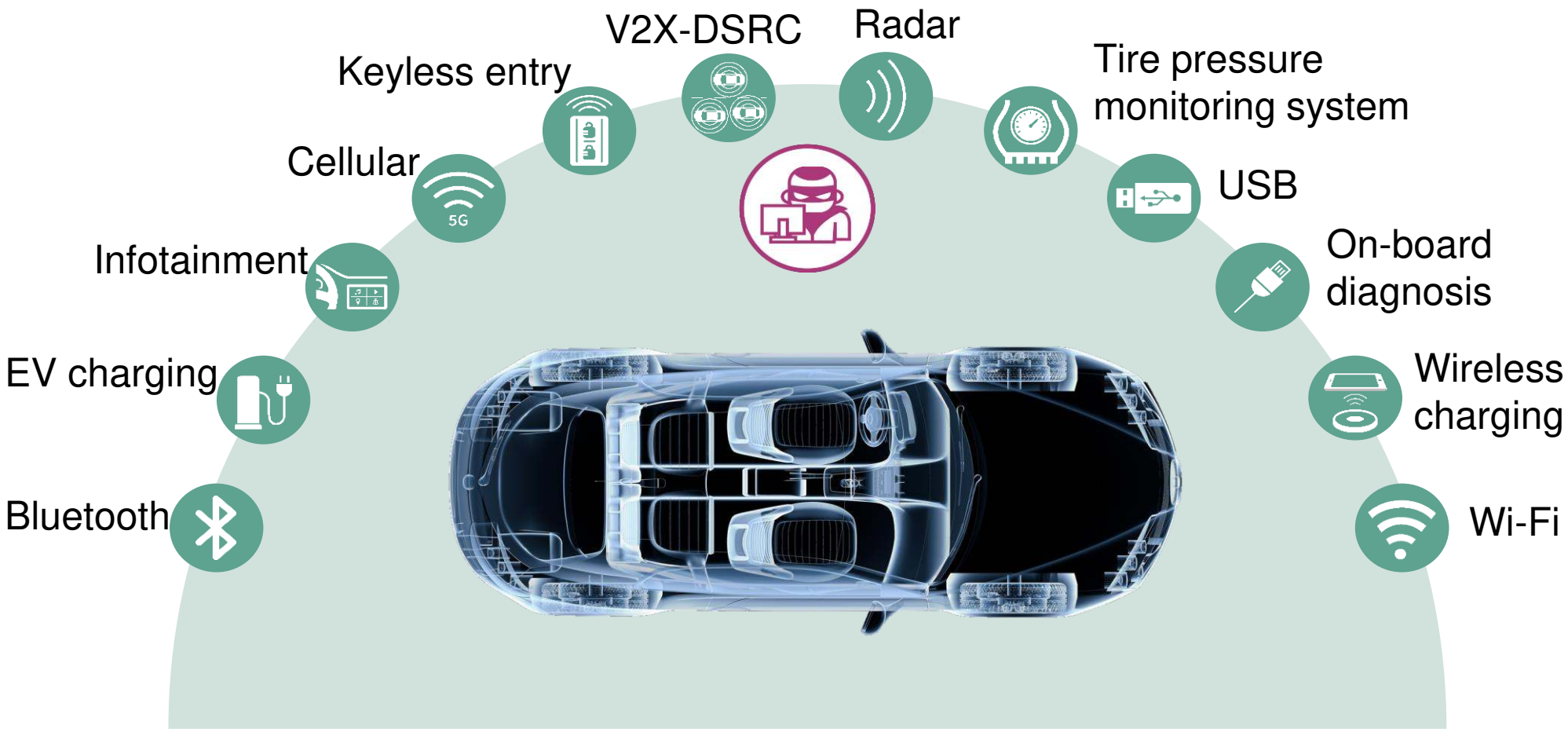
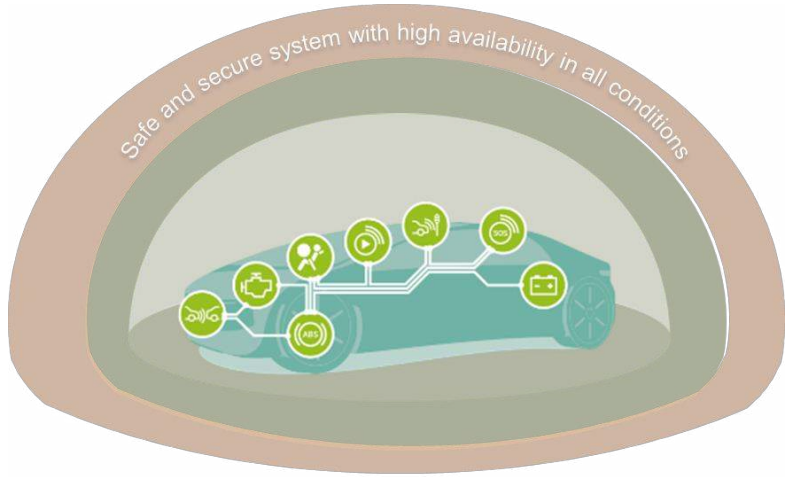


Table of contents

Autonomous vehicle : How to develop highly dependable systems?

High Availability | Ensure high availability beyond critical operations; a safe and secure system, that operates in all conditions



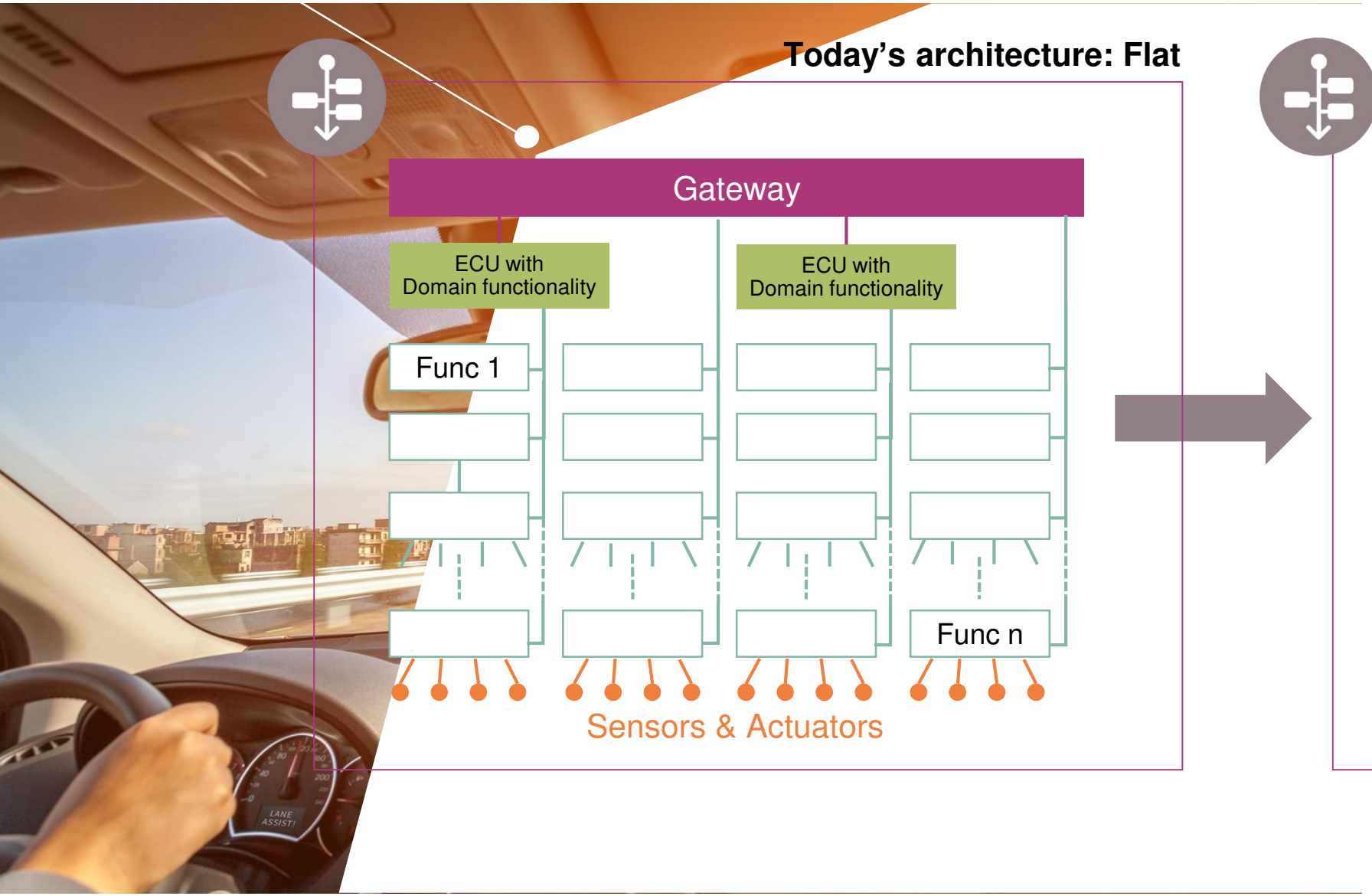
Fail-Operational | Mitigate potentially hazardous effects by ensuring critical operations in the event of a failure

Fail-Safe | in the event of a failure, system enters safe state

	Fail-Safe	Fail-Operational	High Availability
Automation	Lower levels (ADAS, <L2)	Higher levels (AD, ≥L2+)	Higher levels (AD, ≥L3+)
Failure	System enters safe mode	System continues safety critical tasks	High availability in all conditions
System	Reliable, robust, safe, secure	**Fail safe** + available	**Fail operational** + highly available

Table of contents

E/E architecture : How to support next generation E/E architectures?



Today's architecture: Flat

Future architecture: Domain, Zone, or combination

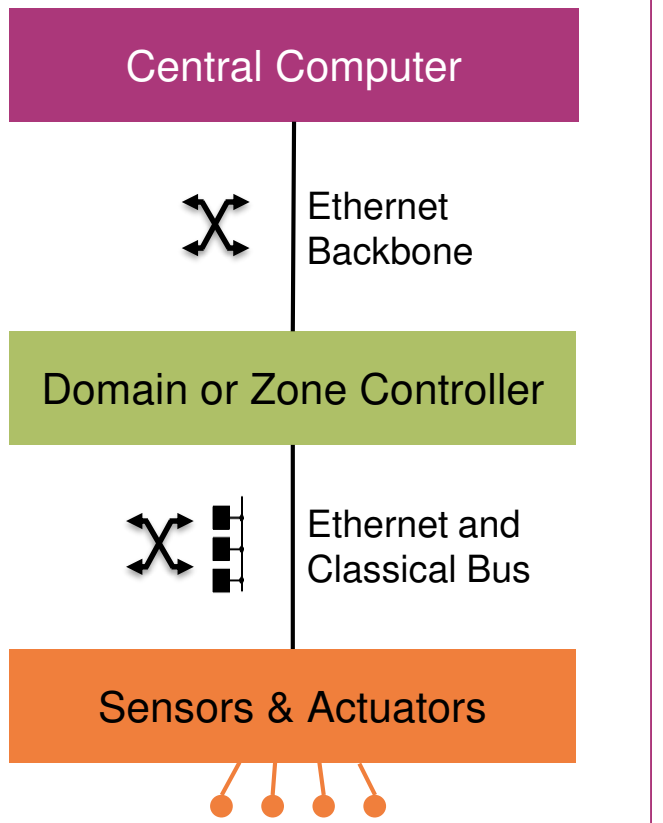


Table of contents

Infineon AURIX™ - the most dependable microcontroller platform

TriCore™ … integration of instructions from three worlds:

RISC, DSP and Real-time

AURIX™ TC4xx.

AURIX™ TC3xx

AURIX™ TC2xx

AUDO MAX

AUDO Future

AUDO Next Gen.

AUDO

TC1.2 40MHz

TC1.3 150MHz

TC1.3.1 180MHz

TC1.6 300MHz

TC1.6.1P Multicore 300MHz

TC1.6.2P Multicore 300MHz

TC 1.8 Multicore 500MHz

…

+FPU

+Cache index
+FPU C convert inst.

+Integer divide
+Code density for Byte&Half-Word

+Multicore
+ Sync. inst

+Improved Memory Hierarchy

+Hypervisor Support
+ 8-stages
+ Double precision floating point

RISC+DSP+Real-time

Performance Increase

2001 2006 2009 2012 2015 2019 2023 **SoP Timeline**

AURIX™ and **TriCore™** means

- Protection of your software investment
- Continuous performance increase
- Continues memory upgrade
- High Scalability

Key improvements with AURIX™ TC4xx

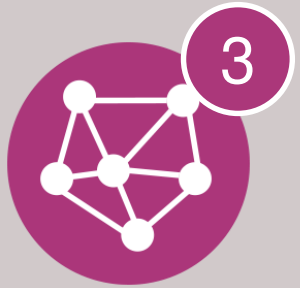
AURIX™ TC4x defines the next controller standard for safe & secure ECUs with strong networking capabilities

Higher Performance

- **New 500MHz TriCore™ 1.8**
- PPU: Private scalar core + **512bit wide vector unit** with up to 72 GOPS
- SPU3: High-performance **radar processing sub-system**
- A/D Converter sub-system **with integrated DSPs**
- **Data Routing Engine** for CAN – Ethernet - Mem communication

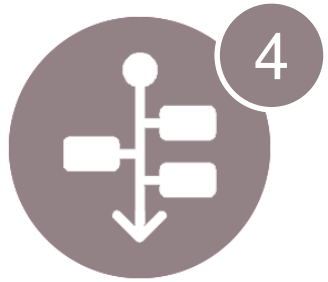
Safety and Security

- AURIX™ meets ISO26262-2018 **ASIL D safety** standard
- **CSRM**: high-performance security module with private CPU, memories and crypto accelerators
- **CSS**: Distributed crypto and hash engines for secure CAN/Ethernet communication
- Security according to **ISO 21434** standard planned



Freedom From Interference

- **Hardware isolation** at core and peripheral level
- TriCore™ 1.8 with **up to eight VMs per core and Hypervisor**
- Ultra-fast **context switching**
- **Enhanced memory protection** for cores and virtual machines
- **Fine-granular access protection** to peripherals
- **Isolated DMA protection**



Rich connectivity

- Up to 2x **5GBit Ethernet** incl. Bridge
- **Accelerated MACsec support** by HW accelerator in CSS and application SW driver
- **4x10/100MBit Ethernet** supporting 10Base-T1S standard
- Up to 2x 8GBit/s **PCIe 3.0** 1x lane
- Up to 20x CAN-FD

AURIX™ TC4x Architecture
Enhancements compared to AURIX™ TC3x

Performance ASIL-D
Enhanced TriCore™
With up to 6CPUs @ **500MHz**

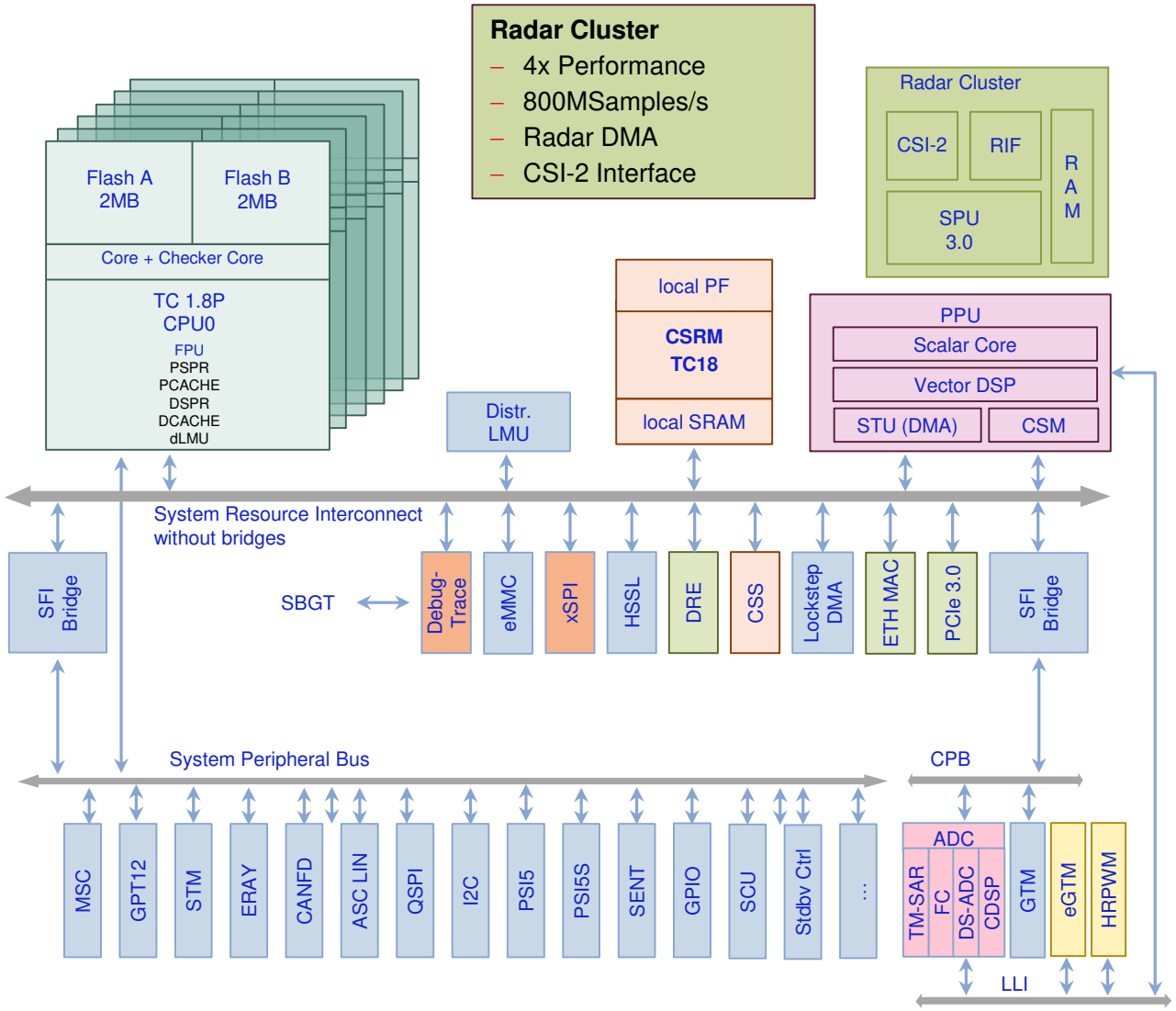
Bigger Tightly Coupled SRAM for increased performance

Full AB-Swap Support

Debug and Trace
Safe and the secure in field

xSPI
External Memory Interface

ADC
Dedicated DSPs
Enhanced ADCs



Radar Cluster
- 4x Performance
- 800MSamples/s
- Radar DMA
- CSI-2 Interface

CSRM
New high performance Security Modules with ASIL-B support

CSS
Dedicated communication security satellites

New Programmable HW Accelerator - PPU
SIMD Vector DSP + Scalar Core for Modelling and Precise Control – **ASIL D**

New high-speed comm Interfaces:
- PCIe 3.0
- 100Mb- 5 Gbps Ethernet

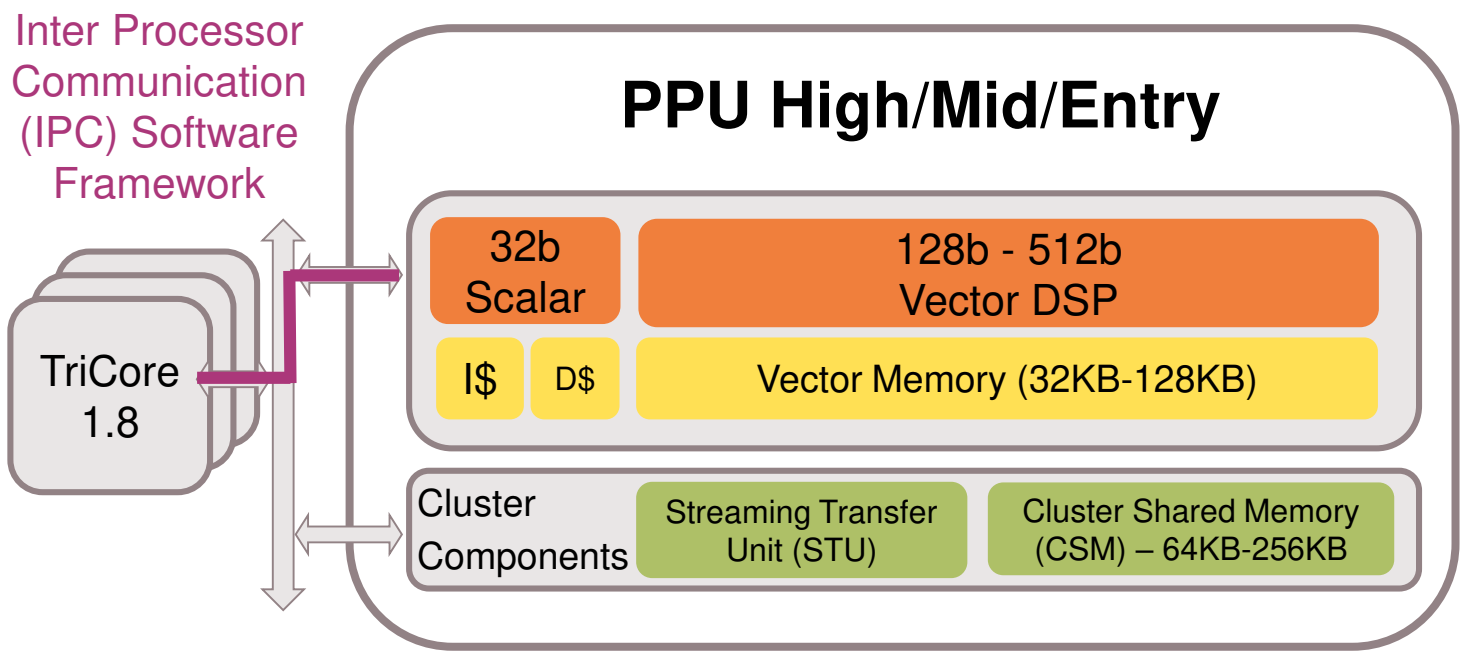
New 10 Mbit Ethernet

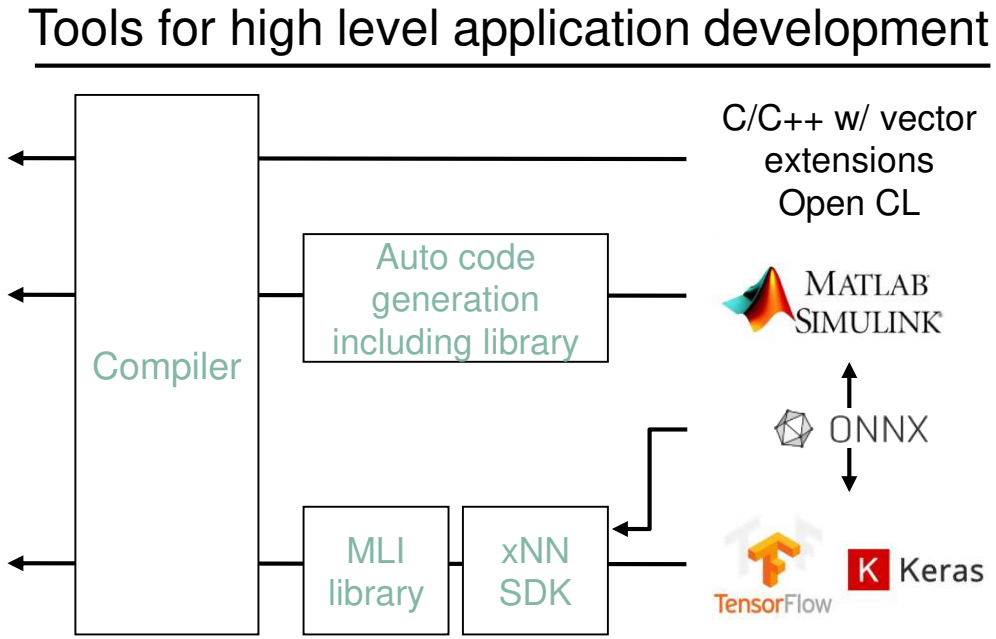
New communication routing accelerator:
- DRE- Data Routing Engine

New eGTM timers and **High Resolution PWM** with **low latency interconnect (LLI)**

Workload specific compute – Machine Learning

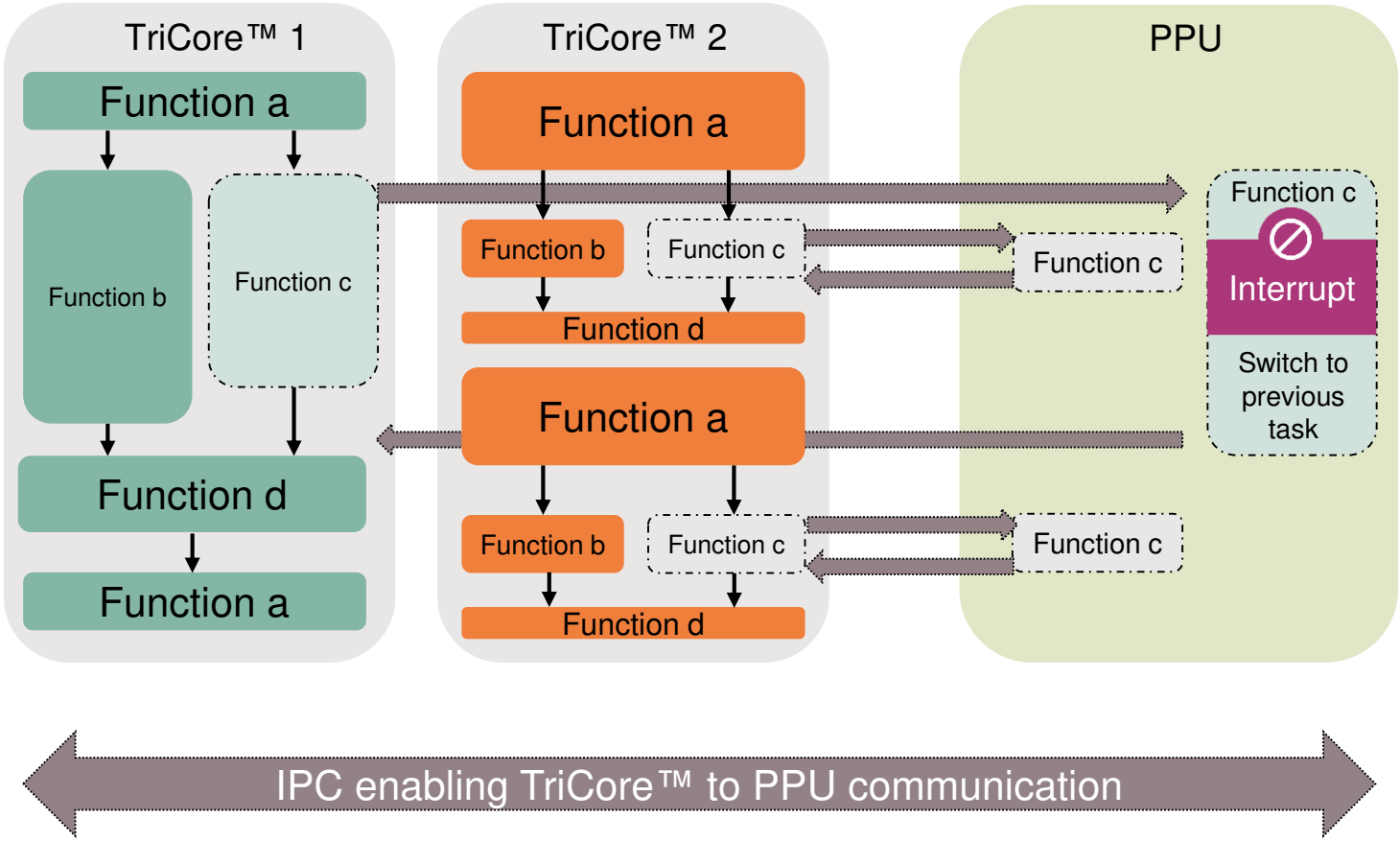
Parallel Processing Unit (PPU): Scalable SIMD Vector DSP





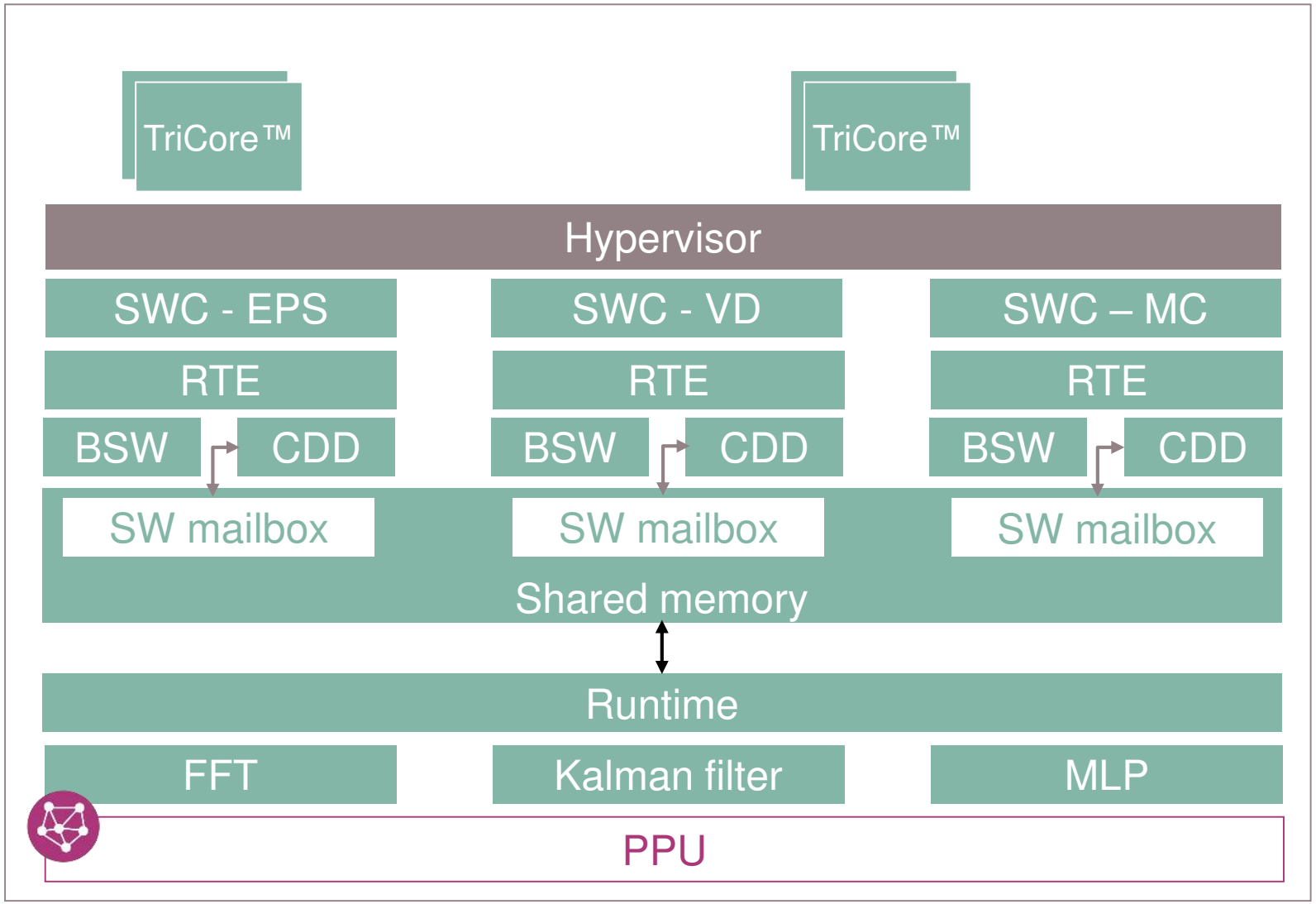
- Scalable PPU EV71FS in TC4x portfolio
- SIMD vector DSP co-processor
- Matrix operation acceleration & data processing
- Neural network based algorithms
- High speed control implementation

Inter processor communication between Tricore™ and PPU



- PPU compute resource will be shared between multiple host CPUs
- Outsourcing of functions into PPU enables speed up of applications tasks
- Middleware is integrated into basic software using complex device driver
- Single level of interruption (priority scheme) is considered

Example: PPU middleware communication with AUTOSAR stack on Tricore™



Example: AUTOSAR Environment

- Three physically isolated AUTOSAR stacks
- Each communicates with PPU using dedicated complex device driver (CDD)
- CDD communicates with middleware on PPU

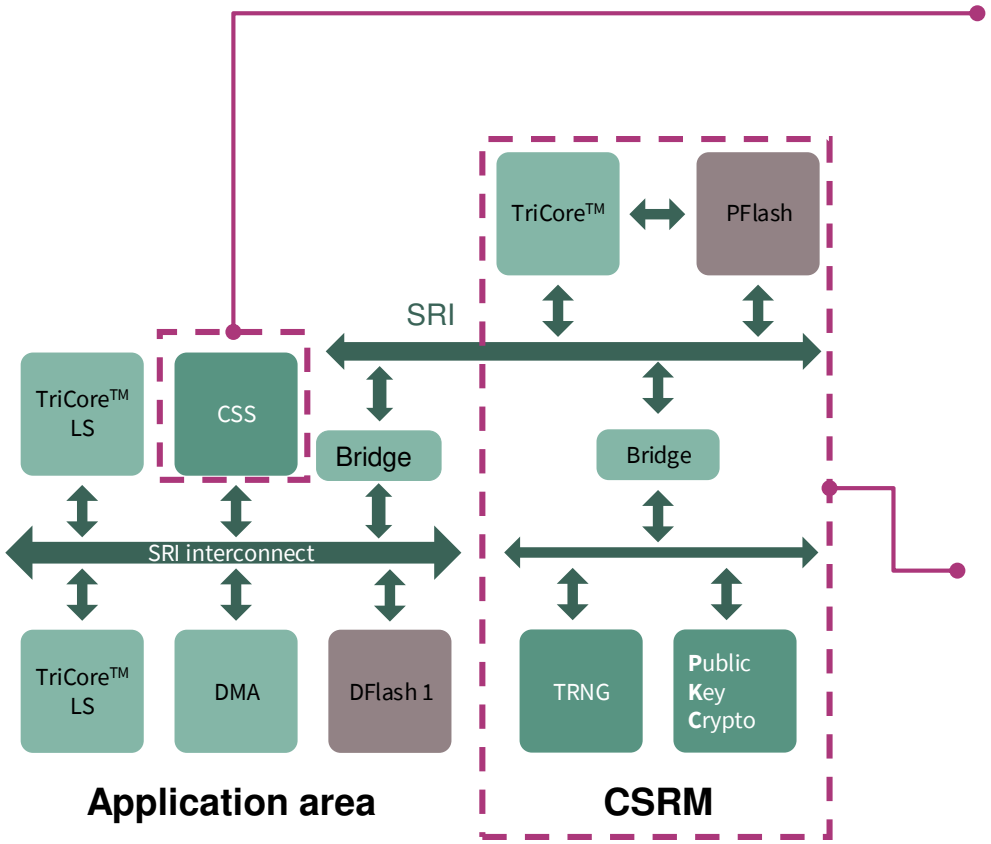
PPU middleware detects requests and executes

- Software on PPU does not differentiate its clients

Security: Hardware acceleration and secure connection to the internet world

Security cluster of AURIX™ TC4x increases throughput by parallel computation and supports upcoming new security standards

New AURIX™ TC4x security cluster



Cyber security satellite (CSS) for parallel computation

- Parallelization of HW accelerators in service provider to application area to avoid performance bottlenecks by
  - Increasing throughput
  - Minimizing latency
- 21 individual channels to be used by application (compared to one channel in TC3x)
- Providing freedom of interference for domain / zone controllers

Cyber security real-time module (CSRM) for performance increase

- Upgrade to TriCore™ 1.8
  - providing ~5-15x more performance vs. TC3x HSM
- CSRM as trusted secure HW environment supporting new security standards (e.g. ISO 21434)
- Private Program Flash within CSRM which supports individual security SW updates independent of application core
- Enables realization of multiple security use cases for wide ranging applications

Security use cases require significantly enhanced performance

Security use cases covered by AURIX™ TC4x

Enabled by SW on CSRM and HW on CSS/PKC/TRNG

- Secure boot
- Debugger protection
- Immobilizer
- Tuning protection
- Secure Update
- Secure (key-) storage
- Component protection
- Key management
- Flight Recorder / Secure Odometer
- Feature Activation
- Remote Diagnosis Car Access (OBD)
- Plug & Charge – OBC (ISO 15118)
- Device Attestation
- Connection to external Service Provider

In-vehicle network (IVN) & V2x (e.g. vehicle to cloud) security

- E/E COM (message) observation:
  - Intrusion Detection System (IDS)
- E/E COM (message) filtering:
  - Intrusion Detection Prevention System (IDPS)
  - Firewall: Feasible by HW filters in MAC and SW
- COM Message Security (e.g. CAN(FD)/Ethernet):
  - Authenticated Encryption with Associated Data (AEAD); Authentication with Associated Data (AAD)
  - Combined modes are supported in CSS

Why is the new security cluster needed?

Minimize latency & maximize throughput as an increasing number of security use cases are expected for the future

Supporting new Security standards (e.g. ISO 21434)

Enable SOTA use cases, which require secure and safe distribution of SW updates from cloud or within IVN

Serve AEAD and AAD solutions, which are expected to gain importance in the future: authentication of >50% and encryption of >15-20% of all IVN messages

Security : Significant performance improvement for AURIX™ TC4xx

Secure Boot[1]

AURIX™TC2x/TC3x
69 MBytes/s
8 MB ~ 120ms

AURIX™ TC4x
Up to 1368 MB/s
24 MB ~ 18ms

20x faster

Faster and less complex startup

[1] CMAC AES-128

SecOC[2]

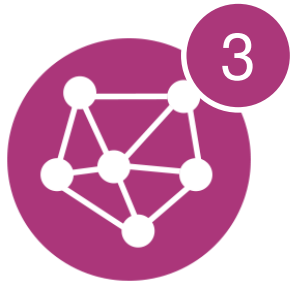
AURIX™TC2x/TC3x
~30 µs

AURIX™ TC4x
0.60µs

50x faster

AURIX™ TC2x/TC3x performance at limit of current project's need
AURIX™ TC4x minimize latency & maximize throughput for future apps

[2] CMAC verify on 16 bytes



Freedom from interference : Safe hardware isolation

Hardware Isolation to separate ASIL and non ASIL applications

Need for Isolation

Example: Zone controller

- Upto 6 per vehicle
- Cross-domain functions in a single ECU

Consolidation of features

- Reduce number of ECUs
- Enhance computing power
- Combine multiple applications with different OS on one MCU

Separation of applications

- Safety: cannot mix safe & unsafe SW
- Security
- Liability: keep SW from partners separate

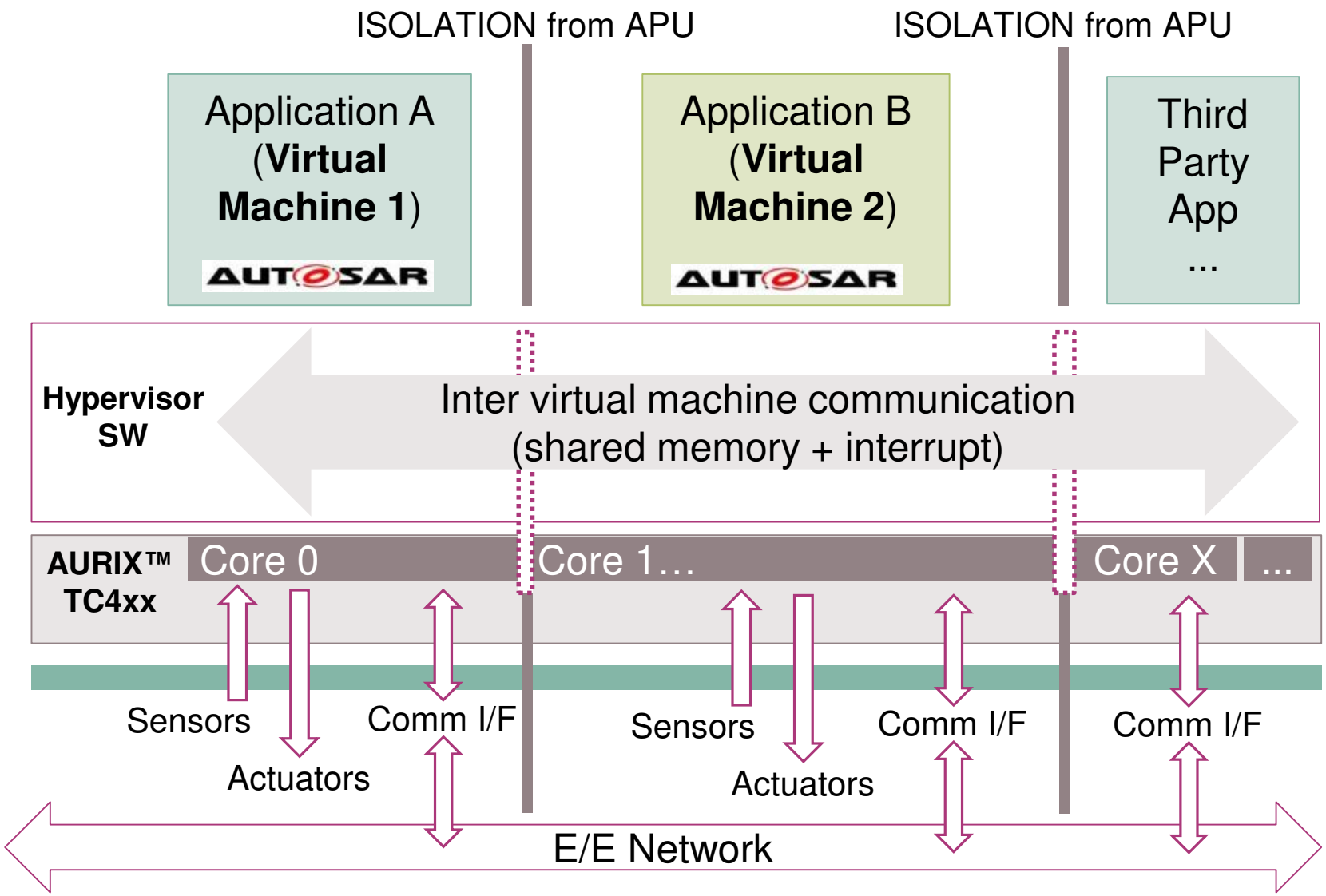
Flexibility

- Enable collaboration from multiple partners
- Separate startup/ shutdown of application
- Independent updates to fix/ upgrade: i.e. OTA
- Monetization: Activate or deactivate features

Introducing Virtual Machines (VM)

- Isolation containers
- Isolates application execution & control path
- One ECU could need upto 30
- Need to be **safe, secure** & **easy to use**

Virtual ECUs deployment using Hypervisor



AURIX™ TC4xx TriCore

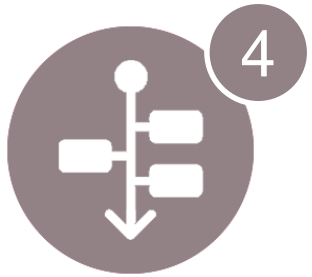
Advanced isolation features at CPU level

Access Protection Unit (APU)

Provides isolation features at the peripherals

Virtual Machines

With complete AUTOSAR stack & assignment of own peripherals

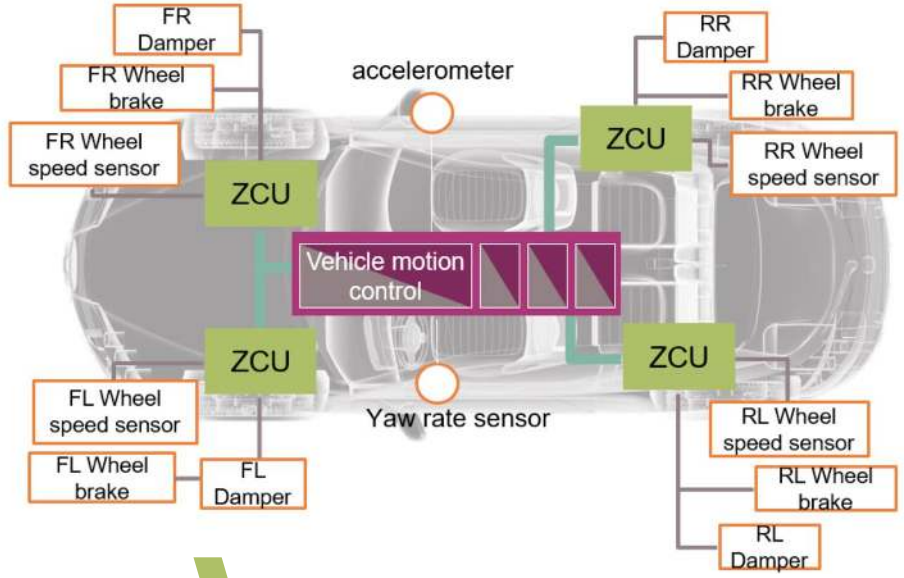


Rich connectivity and low latency data routing

Feature set deep dive: Rich connectivity
TC4xx meets the latency and ethernet performance challenges

Challenge:
Latency when sharing real time data i.e. wheel sensor between zone controllers

TC4xx DRE/CRE routing accelerators:
- Reduces SW processing load of data transmission
- Increase performance and throughput
- by reducing routing latency and jitter
- Use-cases covered:
  - Packet forwarding CAN←→CAN
  - Packet formatting and encapsulation CAN←→ETH
  - Packet storage CAN→Memory



Challenge:
Ethernet bridge performance & redundancy for safety critical application in daisy chain & ring topologies

TC4xx Ethernet MACs and Ethernet bridge:
- High-speed Ethernet with TSN support
- Combo MAC with 100Mbps and 10BaseT1s support
- Ethernet bridge with filter and parser capabilities

Reduces communication load on CPUs and enables safety critical real time communication

Comprehensive ethernet and CAN connectivity and feature set to address wide variety of future IVN demands

2 x 5 Gbps MAC

Supported speeds:

- 100Mbps (MII,RMII, RGMII)
- 1Gbps(RGMII, SGMII)
- 2.5Gbps (SGMII)
- 5Gbps (SGMII)

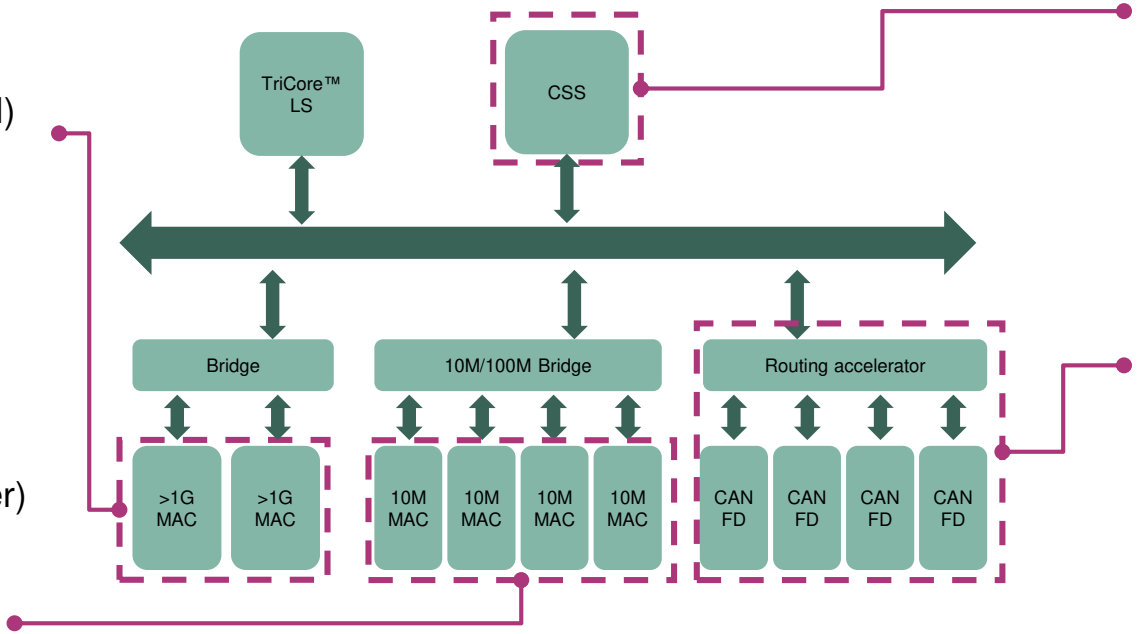
4 x 10/100 Mbps MAC

Supported speeds:

- 100Mbps (MII, RMII)
- 10Mbps (3 Pin Transceiver)

Supported topologies:

- point-to-point (100M)
- Bus (10M)



CSS - Security Accelerator

Supports security algorithms for

- MACsec
- IPsec
- D/TLS
- SecOC (PDU level)

20 x CAN-FD nodes and routing engine

- CAN-to-CAN frame routing across all 20 CAN channels
- CAN-to-Memory frame routing
- CAN-to-Ethernet routing (IEEE:1722 support)
- Multi-cast up to 4 destinations
- Intrusion Detection support
- Virtualization support

Ethernet MAC Features

- **Quality of service**: provides queues for frames
- **Classification**: applies rules to inbound packets
- **TSN**: provides functions to achieve real time behavior
- **Intrusion detection**: supports detection of anomalies
- **Bridge**: support fast forwarding of frames

Software Ecosystem

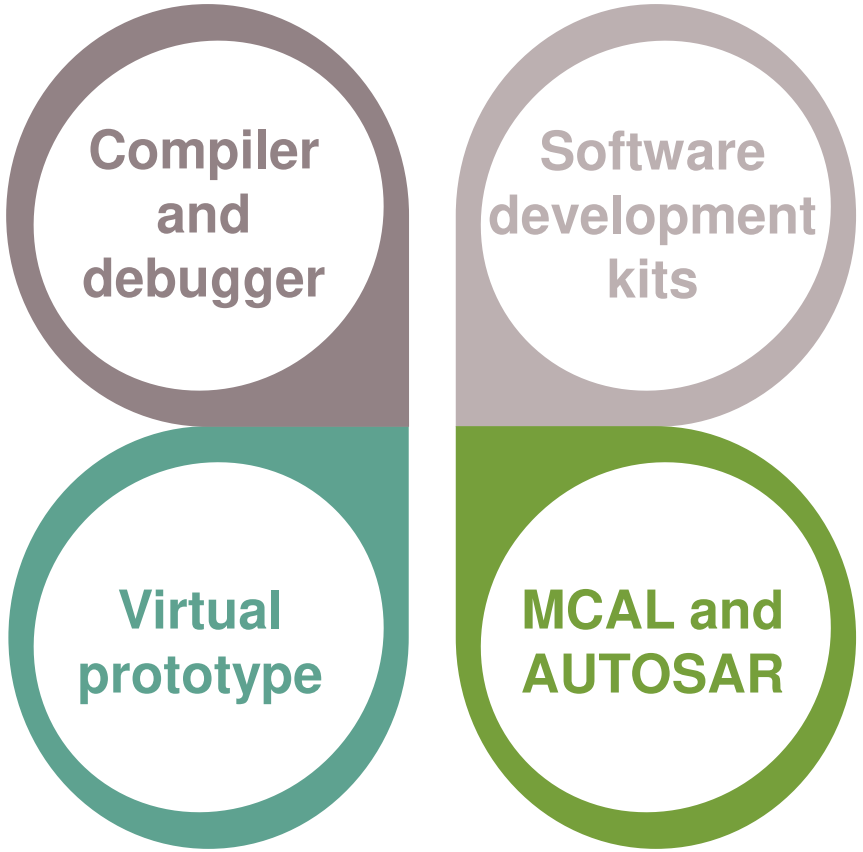
Getting started with new SDKs and re-using proven ecosystem

Last generation re-use plus support of new computing IP

- **TriCore™ compiler:**
  - TASKING, Hightec, WindRiver, GHS
- **PPU compiler:**
  - Synopsys, TASKING, Hightec
- **Debugger and test tools:**
  - iSYSTEM, Lauterbach, PLS, Synopsys

Enablement of pre-silicon development

- **Provider:** Synopsys
- Modelling of key AURIX TC4x HW features
- Full debug and analysis support
- Interfaces to Simulink, SABER, CANoe, etc.



Enabling development with new IP plus increased safety support

- **PPU libraries and auto code generation:**
  - Synopsys, TASKING
- **AURIX TC4x hardware support package**
  - MATLAB / Simulink
- **Safety software package *(in discussion)***
  - Startup tests and failure checks recommended in safety manual
- **Optional CDSP software toolchain**
  - Synopsys

Increased MCAL offering and AUTOSAR providers incl. hypervisor

- Proprietary MCAL with ISO26262:2018 compliance for IPs incl. new COM Ips (PCIe, DRE, 10BaseT1s)
- **Hypervisor implementation**
  - EB, ETAS, Opensynergy, SysGo, Greenhills
- **SW stack integration providers:**
  - Vector, Elektrobit, Siemens, ETAS
- **Security SW:** Vector, ESCRYPT, ISS, EB

Table of contents

Example ADAS use case : Autonomous L1/L2 Sensor Fusion

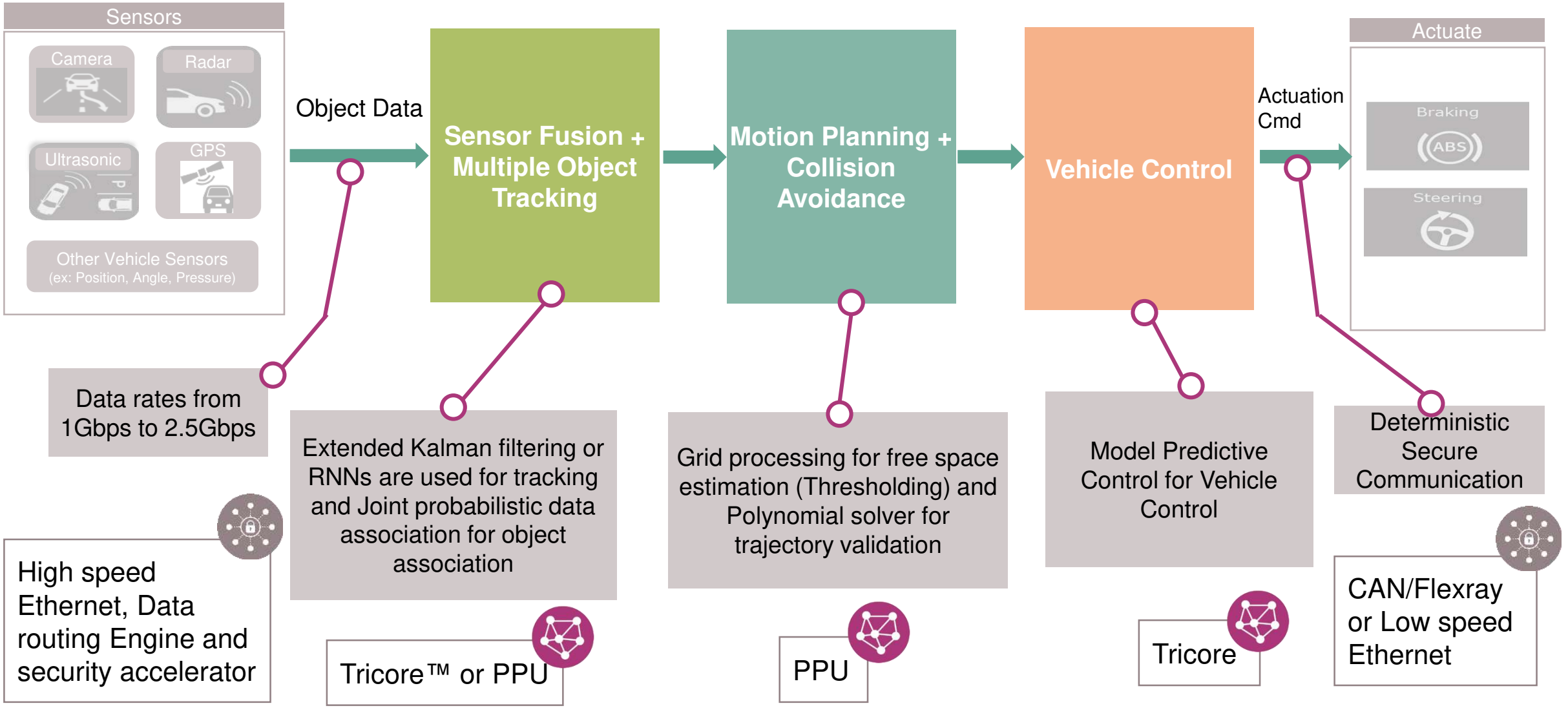


Table of contents

AURIX™ TC4xx Heterogeneous SoC architecture enabling highest level of safety for automotive applications

- E/E architecture evolution
- High availability beyond critical operations
- Connectivity to “world" needs high security
- Higher workload specific compute

AURIX™ Microcontrollers

ISO 26262 compliant

CPU + accelerators

Performance

- Cyber Security Accelerator — Security
- Data Routing Engine — Faster data processing
- Signal Processing Unit — Sensor processing
- Parallel Processing Unit — Machine learning
- TriCore™ CPU — ASIL-D processing

ASIL D:
~8k DMIPS+
72GFlops
+
ASIL-B:
1.2k DMIPS

ASIL Performance

Summary : AURIX™ TC4xx enables heterogeneous computing with industry leading functional safety concept

AURIX™ TC4xx offers tremendous computational power boost compared to previous generation deploying new applications with complex computing needs

Optimized SoC with high speed connectivity, data routing engine, hypervisor for isolation to enable next generation EE architectures

Scalable and flexible Parallel Processing Unit (PPU) enables affordable artificial intelligence with its high performance SIMD architecture

Holistic functional safety concept with improved safety mechanisms, Security cluster supporting security standards and with significantly enhanced performance

AURIX™ TC4xx offers a scalable platform from low end to high devices enabled with rich software ecosystem to support the next generation of mobility

Part of your life. Part of tomorrow.