Heterogeneous computing to enable highest level of safety

Ramanujan Venkatadri
Automotive Innovation Center, Infineon Technologies
# Table of contents

<table>
<thead>
<tr>
<th></th>
<th>Challenges to address next generation automotive systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
# Table of contents

1. Challenges to address next generation automotive systems
   - 3
2. Exponential increase in workload specific compute
   - 5
3. How to secure the future connected vehicle?
   - 7
4. How to achieve higher levels of autonomy?
   - 9
5. How to address the new EE architecture challenges
   - 11
6. Introduction to next generation AURIX TC4xx microcontrollers
   - 13
7. Example application use case
   - 29
8. Summary
   - 31
Challenges with developing autonomous, electric and connected Vehicle

- Connected, Autonomous Electric Mobility
- Evolving technologies (ex: Battery, Sensing, and AI)
- E/E architecture evolution
- High availability beyond critical operations
- Connectivity to “world” needs high security
- Higher workload specific compute
<table>
<thead>
<tr>
<th>1</th>
<th>Challenges to address next generation automotive systems</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
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

1. Challenges to address next generation automotive systems 3
2. Exponential increase in workload specific compute 5
3. How to secure the future connected vehicle? 7
4. How to achieve higher levels of autonomy? 9
5. How to address the new EE architecture challenges 11
6. Introduction to next generation AURIX TC4xx microcontrollers 13
7. Example application use case 29
8. Summary 31
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

1. Challenges to address next generation automotive systems  
2. Exponential increase in workload specific compute  
3. How to secure the future connected vehicle?  
4. How to achieve higher levels of autonomy?  
5. How to address the new EE architecture challenges  
6. Introduction to next generation AURIX TC4xx microcontrollers  
7. Example application use case  
8. Summary
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.

- Lower levels (ADAS, <L2)
- System enters safe mode
- Reliable, robust, safe, secure

- Higher levels (AD, ≥L2+)
- System continues safety critical tasks
- Fail safe + available

- Higher levels (AD, ≥L3+)
- High availability in all conditions
- Fail operational + highly available
# Table of contents

<table>
<thead>
<tr>
<th></th>
<th>Challenges to address next generation automotive systems</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
E/E architecture: How to support next generation E/E architectures?

Today's architecture: Flat

Future architecture: Domain, Zone, or combination

Central Computer
- Ethernet Backbone

Domain or Zone Controller
- Ethernet and Classical Bus

Sensors & Actuators

Gateway
- ECU with Domain functionality
- Func 1
- Func n
<table>
<thead>
<tr>
<th></th>
<th>Challenges to address next generation automotive systems</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
Infineon AURIX™ - the most dependable microcontroller platform

TriCore™ … integration of instructions from three worlds:
RISC, DSP and Real-time

TC1.2
40MHz

TC1.3
150MHz

TC1.3.1
180MHz

TC1.6
300MHz

TC1.6.1P
Multicore 300MHz
+Integer divide
+Sync. inst
+Multicore

TC1.6.2P
Multicore 500MHz
+Hypervisor Support
+8-stages
+Double precision floating point
+Improved Memory Hierarchy

AURIX™
TC2xx

AUDO Future

AUDO MAX

AUDO Next Gen.

TC1.8
Multicore 500MHz

AURIX™
TC3xx

AURIX™
TC4xx.

AUDO

TC 1.8
Multicore 500MHz

+Hypervisor Support
+8-stages
+Double precision floating point
+Improved Memory Hierarchy

AURIX™ and TriCore™ means
› Protection of your software investment
› Continuous performance increase
› Continues memory upgrade
› High Scalability

SoP Timeline
Key improvements with AURIX™ TC4xx
AURIX™ TC4x defines the next controller standard for safe & secure ECUs with strong networking capabilities

1. **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

2. **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

3. **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

4. **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 6 CPUs @ 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

PPU High/Mid/Entry

- 32b Scalar
- 128b - 512b Vector DSP
- I$ D$
- Vector Memory (32KB-128KB)
- Streaming Transfer Unit (STU)
- Cluster Shared Memory (CSM) – 64KB-256KB

TriCore 1.8

Tools for high level application development

- C/C++ w/ vector extensions
- Open CL
- MATLAB SIMULINK
- ONNX
- MLI library
- xNN SDK
- Auto code generation including library
- Compiler
- Inter Processor Communication (IPC) Software Framework
- Compiler
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

IPC enabling TriCore™ to PPU communication
Example: PPU middleware communication with AUTOSAR stack on TriCore™

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

<table>
<thead>
<tr>
<th>Enabled by SW on CSRM and HW on CSS/PKC/TRNG</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>› Secure boot</td>
<td>› Flight Recorder / Secure Odometer</td>
</tr>
<tr>
<td>› Debugger protection</td>
<td>› Feature Activation</td>
</tr>
<tr>
<td>› Immobilizer</td>
<td>› Remote Diagnosis Car Access</td>
</tr>
<tr>
<td>› Tuning protection</td>
<td>(OBD)</td>
</tr>
<tr>
<td>› Secure Update</td>
<td>› Plug &amp; Charge – OBC (ISO 15118)</td>
</tr>
<tr>
<td>› Secure (key-) storage</td>
<td>› Device Attestation</td>
</tr>
<tr>
<td>› Component protection</td>
<td>› Connection to external Service</td>
</tr>
<tr>
<td>› Key management</td>
<td>Provider</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>In-vehicle network (IVN) &amp; V2x (e.g. vehicle to cloud) security</th>
</tr>
</thead>
<tbody>
<tr>
<td>› E/E COM (message) observation:</td>
</tr>
<tr>
<td>‹ Intrusion Detection System (IDS)</td>
</tr>
<tr>
<td>› E/E COM (message) filtering:</td>
</tr>
<tr>
<td>‹ Intrusion Detection Prevention System (IDPS)</td>
</tr>
<tr>
<td>‹ Firewall: Feasible by HW filters in MAC and SW</td>
</tr>
<tr>
<td>› COM Message Security (e.g. CAN(FD)/Ethernet):</td>
</tr>
<tr>
<td>‹ Authenticated Encryption with Associated Data (AEAD);</td>
</tr>
<tr>
<td>‹ Authentication with Associated Data (AAD)</td>
</tr>
<tr>
<td>‹ Combined modes are supported in CSS</td>
</tr>
</tbody>
</table>

### 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 Boot¹

- 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

SecOC²

- 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

¹ CMAC AES-128
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

Application A (Virtual Machine 1)

Application B (Virtual Machine 2)

Third Party App ...

Hypervisor SW

Inter virtual machine communication (shared memory + interrupt)

Core 0

Core 1 ...

Core X ...

AURIX™ TC4xx

Core X ...

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

Copyright © Infineon Technologies AG 2021. All rights reserved.
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

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, ECRYPT, ISS, EB
# Table of contents

<table>
<thead>
<tr>
<th></th>
<th>Challenges to address next generation automotive systems</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
Example ADAS use case: Autonomous L1/L2 Sensor Fusion

**Sensors**
- Camera
- Radar
- Ultrasonic
- GPS
- Other Vehicle Sensors (ex: Position, Angle, Pressure)

**Object Data**

**Sensor Fusion + Multiple Object Tracking**
- Data rates from 1Gbps to 2.5Gbps
- High speed Ethernet, Data routing Engine and security accelerator

**Motion Planning + Collision Avoidance**
- Extended Kalman filtering or RNNs are used for tracking and Joint probabilistic data association for object association
- Grid processing for free space estimation (Thresholding) and Polynomial solver for trajectory validation

**Vehicle Control**
- Model Predictive Control for Vehicle Control
- Deterministic Secure Communication

**Actuation**
- Braking (ABS)
- Steering
- CAN/Flexray or Low speed Ethernet

**Actuate**
- Tricore™ or PPU
- PPU
- Tricore

Copyright © Infineon Technologies AG 2021. All rights reserved.
# Table of contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Challenges to address next generation automotive systems</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Exponential increase in workload specific compute</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How to secure the future connected vehicle?</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>How to achieve higher levels of autonomy?</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>How to address the new EE architecture challenges</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Introduction to next generation AURIX TC4xx microcontrollers</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Example application use case</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Summary</td>
<td>31</td>
</tr>
</tbody>
</table>
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

CPU + accelerators

Cyber Security Accelerator

Data Routing Engine

Signal Processing Unit

Parallel Processing Unit

TriCore™ CPU

ASIL-D:
~8k DMIPS+
72GFlops

ASIL-B:
1.2k DMIPS

Performance

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

ASIL Performance

ISO 26262 compliant
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
infineon

Part of your life. Part of tomorrow.