hitex

AURIX KNOWLEDGE LAB 2024

ETAS HIGHTEC imagimob An Infineon Technologies Company

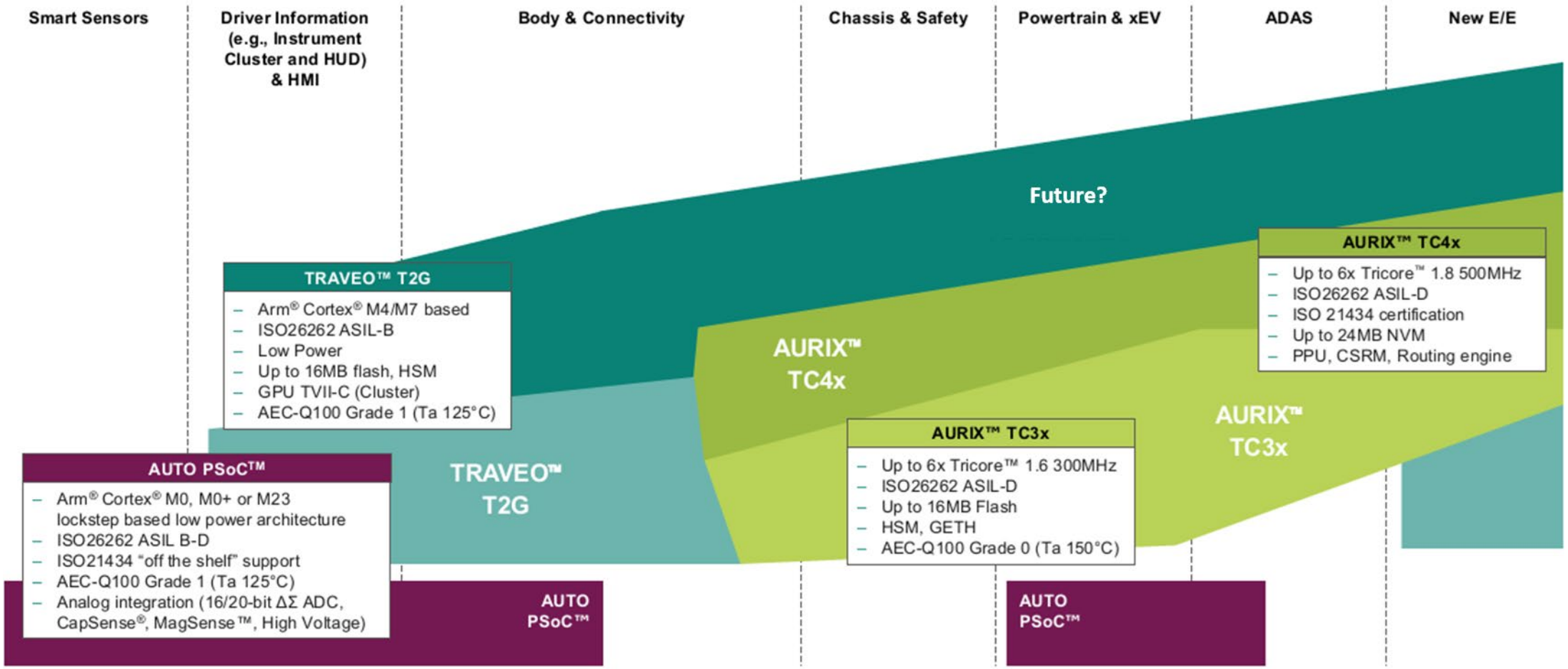
Infineon pls Development Tools TRUST IN SOFT

What's new and special with TC4x

Matthias Spranz, Head of Engineering

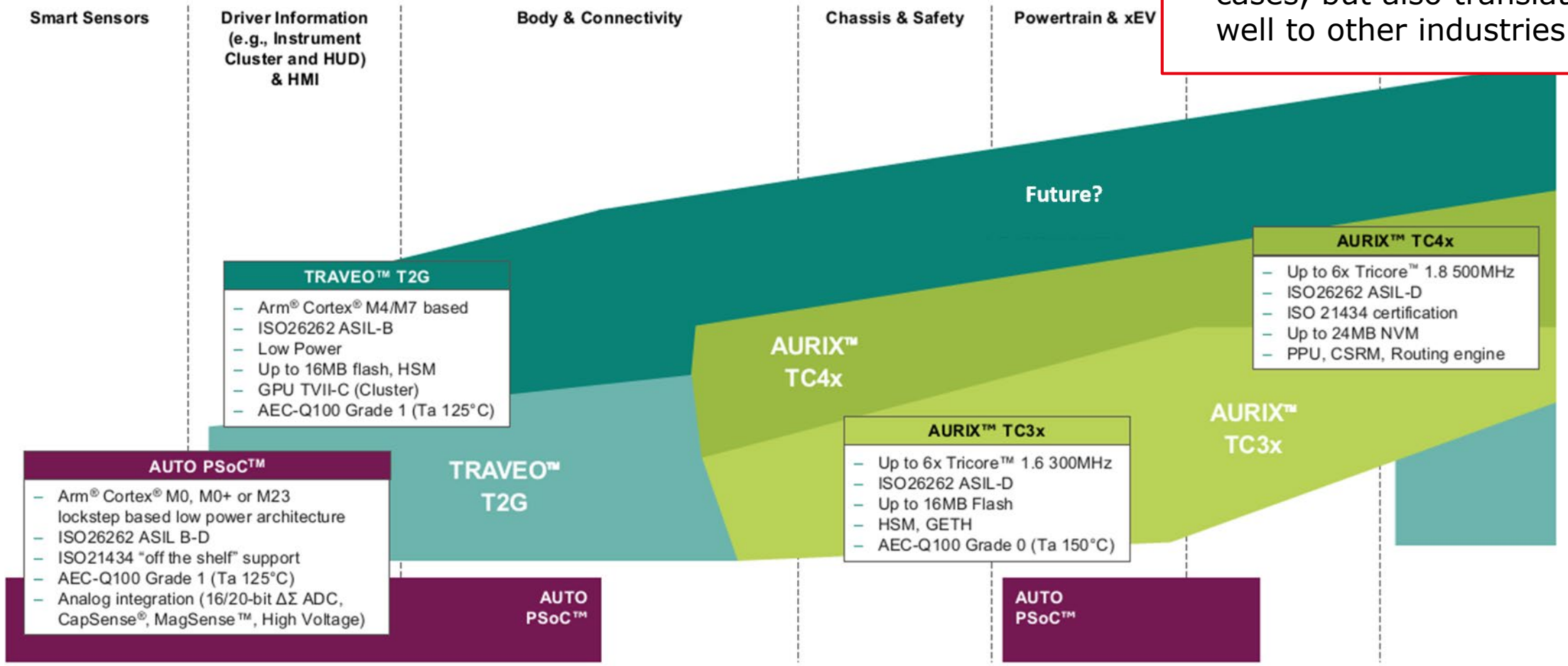
hitex EMBEDDED TOOLS & SOLUTIONS

Infineon µC range and where TC4x fits in



Infineon µC range and where TC4x fits in

(i) Note: Automotive use cases, but also translates well to other industries



TC4x, next controller standard for safe and secure ECUs with strong networking capabilities?

hitex
EMBEDDED TOOLS & SOLUTIONS

Higher Performance

- **New 500MHz TriCore™ 1.8**
- PPU: Private scalar core + **256bit wide vector unit** with up to 48 GOPS
- SPU3: High-performance **radar processing sub-system**
- A/D Converter sub-system **with integrated DSPs**
- **Data Routing Engine** for CAN – Ethernet - Mem communication
- Improved Timers, HR-PWM

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

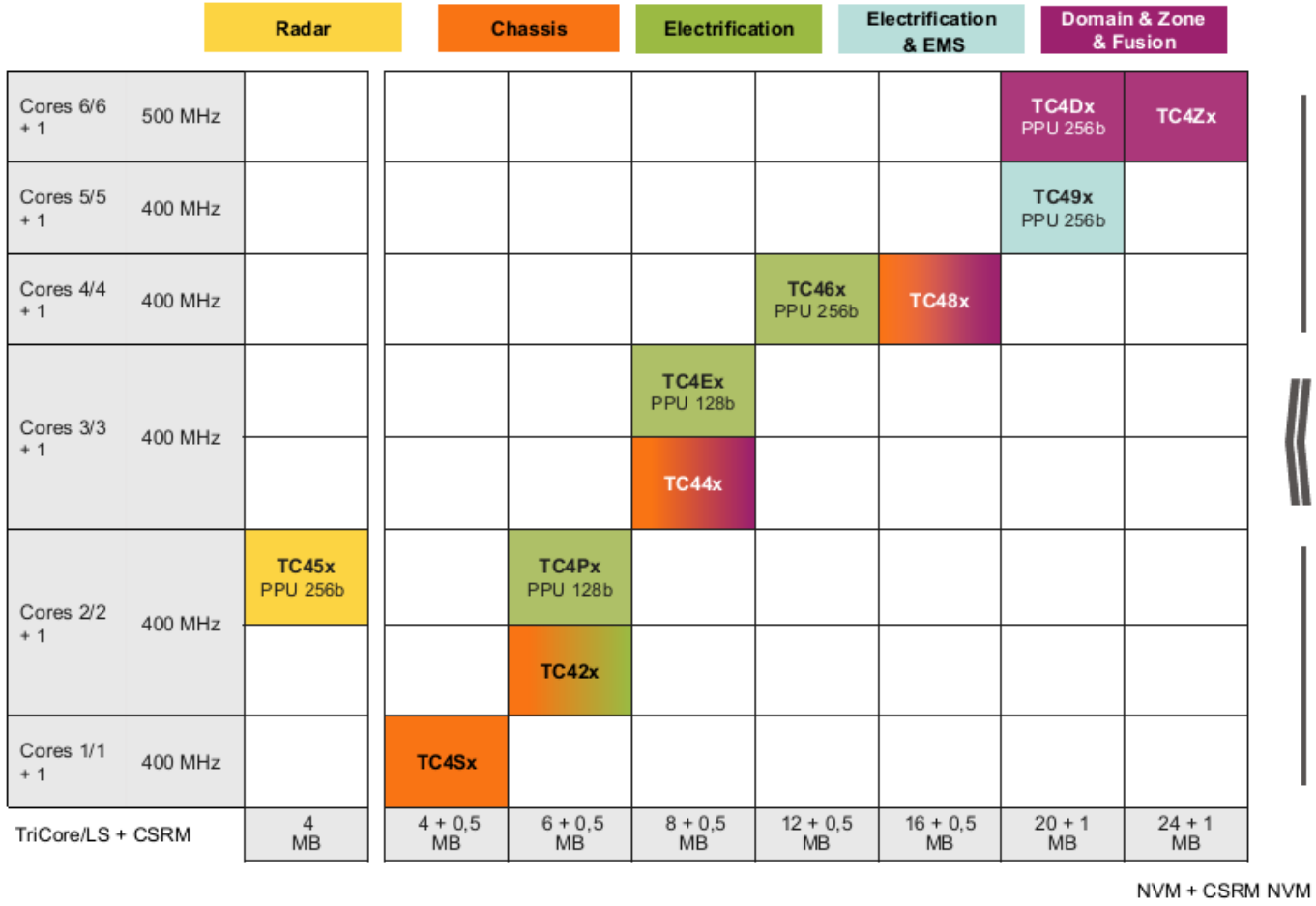
- **Hardware isolation** at core and peripheral level
- TriCore™ 1.8 with **up to eight VMs per core and Hypervisor**
- Ultra-fast **context switching**
- **Enhanced memory protection** for cores and virtual machines
- **Fine-granular access protection** to peripherals
- **Isolated DMA protection**

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
- **CAN-XL**

Productive devices and main applications

› Productive devices & main applications



TC4x enhancements

Performance increase
Up to 500 MHz

Parallel Processing Unit (PPU)
to drive further innovation like virtual sensors and MPC**

Cutting edge security features
to protect with future Post-Quantum Cryptography, ISO/SAE 21434 certified process

Hypervisor to combine
many applications on one MCU and to enable SW-sharing on one Core with ensured FFI**

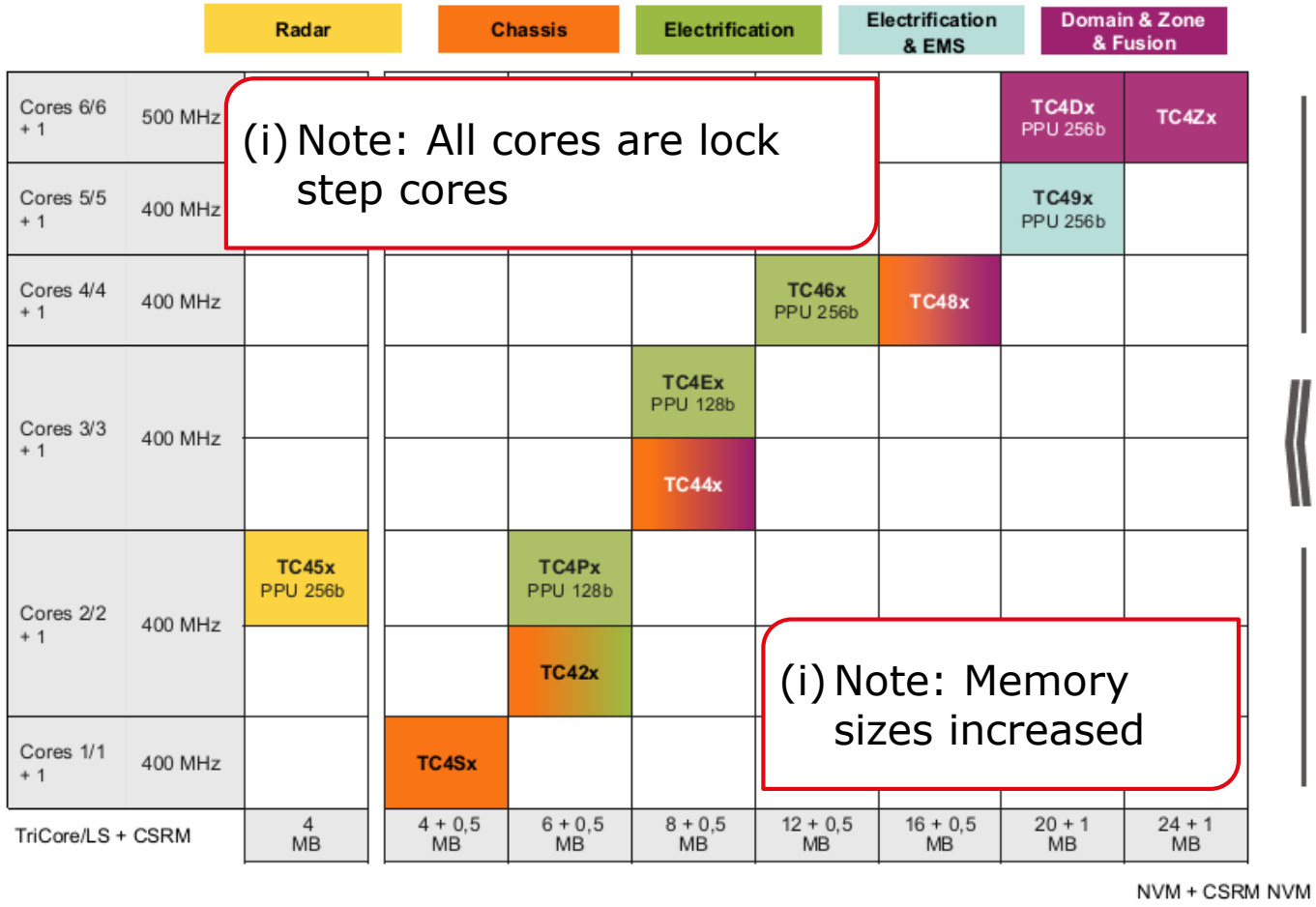
Next Level of Communication
up to 5 Gbit/s ETH,PCIe

Model-based SW development
TC4x Hardware-Support-package

**Model Predictive Control, FFI = Freedom For Interference

Productive devices and main applications

› Productive devices & main applications



TC4x enhancements

Performance increase
Up to 500 MHz

Parallel Processing Unit (PPU)
to drive further innovation like virtual sensors and MPC**

Cutting edge security features
to protect with future Post-Quantum Cryptography, ISO/SAE 21434 certified process

Hypervisor to combine many applications on one MCU and to enable SW-sharing on one Core with ensured FFI**

Next Level of Communication
up to 5 Gbit/s ETH,PCIe

Model-based SW development
TC4x Hardware-Support-package

**Model Predictive Control, FFI = Freedom For Interference

TC4x package types – two main variants for different application needs

hitex
EMBEDDED TOOLS & SOLUTIONS

(i) Note: Same pinout in the same package → move up or down during development

	Standard Pinout						COM Pinout		
TC4Zx Cores 6/6+1 @500MHz 24+1 MB								**TC4Z7** SAK	**TC4Z9** SAK
TC4Dx Cores 6/6+1 @500MHz 20+1 MB and PPU								**TC4D7** SAA / SAK*	**TC4D9** SAA / SAK*
TC49x Cores 5/5+1 @400MHz 20+1 MB and PPU					**TC497** SAK	**TC499** SAK			
TC48x Cores 4/4+1 @400MHz 16+0.5 MB				**TC486** SAK	**TC487** SAK			**TC487** SAK	**TC489** SAK
TC46x Cores 4/4+1 @400MHz 12+0.5 MB				**TC466** SAK	**TC467** SAK	**TC469** SAK			
TC4Ex Cores 3/3+1 @400MHz 8+0.5 MB and PPU				**TC4E6** SAK	**TC4E7** SAK				
TC44x Cores 3/3+1 @400MHz 8+0.5 MB			**TC445** SAK	**TC446** SAK	**TC447** SAK		**TC445** SAK	**TC447** SAK	
TC4Px Cores 2/2+1 @400MHz 6+0.5 MB and PPU			**TC4P5** SAK	**TC4P6** SAK	**TC4P7** SAK				
TC42x Cores 2/2+1 @400MHz 6+0.5 MB	**TC422** SAK	**TC423** SAK	**TC425** SAK	**TC426** SAK	**TC427** SAK				
TC4Sx Cores 1/1+1 @400MHz 4+0.5 MB	**TC4S2** SAK	**TC4S3** SAK	**TC4S5** SAK	**TC4S6** SAK	**TC4S7** SAK				
	TQFP100	TQFP144	BGA188	BGA224	BGA292	BGA436	BGA188	BGA292	BGA436
Dimensions | Pitch [mm]	12x12 | 0.4	16x16 | 0.4	12x12 | 0.8	14x14 | 0.8	17x17 | 0.8	21x21 | 0.8	12x12 | 0.8	17x17 | 0.8	21x21 | 0.8

Temperature

SAA	T_A up to 105 ° C / T_j up to 145 ° C
SAK	T_A up to 125 ° C / T_j up to 160 ° C

* TC4Dx SAK limited to T_J up to 145 ° C

Standard Pinout

› Optimized legacy pinout to address smart actuators market like Chassis, Electrification & Engine Management

Communication Pinout

› Defined for Domain, Zone, gateway, SF and camera controller applications.

› Enable high speed communication interfaces (like 5 Gbit Ethernet and PCIe)

All devices shown are Overmolded. Alternative cooling options may be available depending on device and package selected

Architecture Enhancements compared to TC3x

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

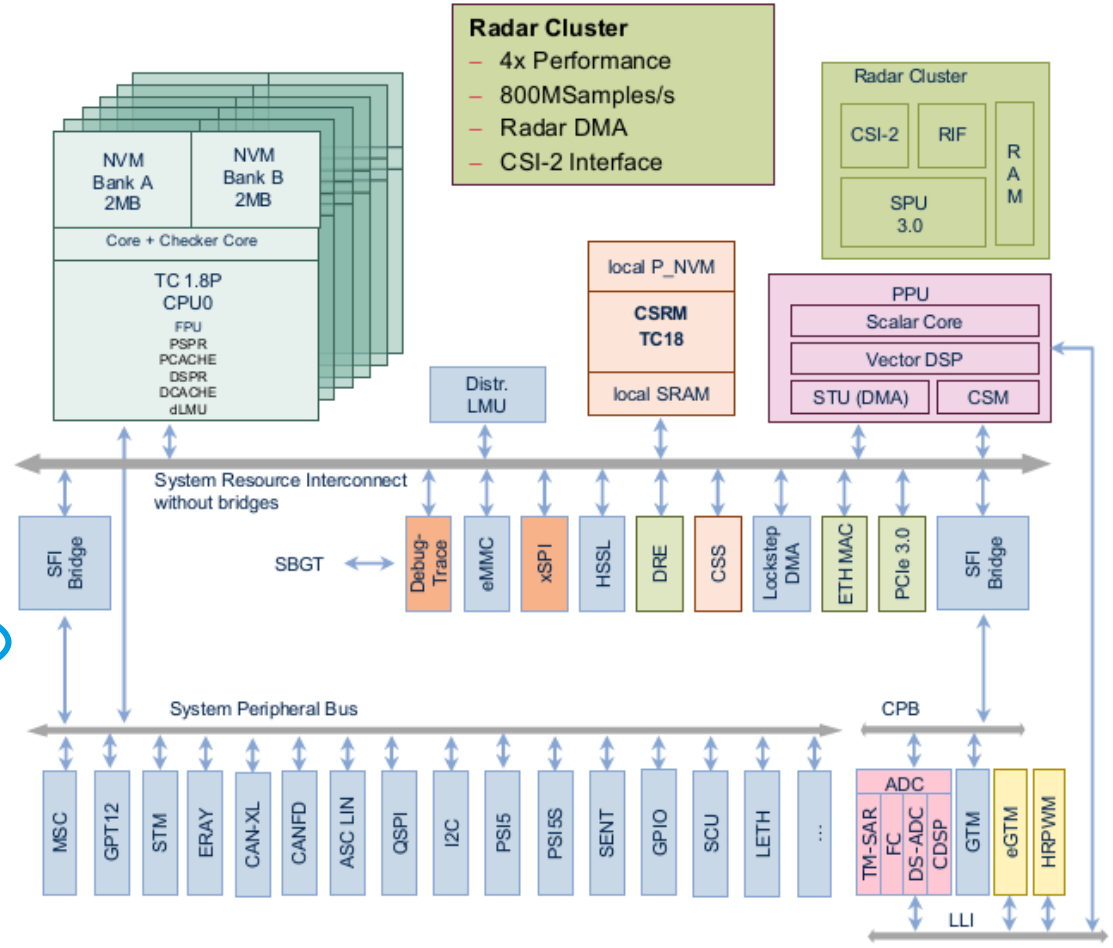
Bigger Tightly Coupled SRAM for increased performance

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 QM 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 and CAN-XL

New communication routing accelerator:
- DRE- Data Routing Engine

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

Architecture Enhancements compared to TC3x

(i) Note: same access time for A and B swapped partition

With up to 6CPUs @ **500MHz**

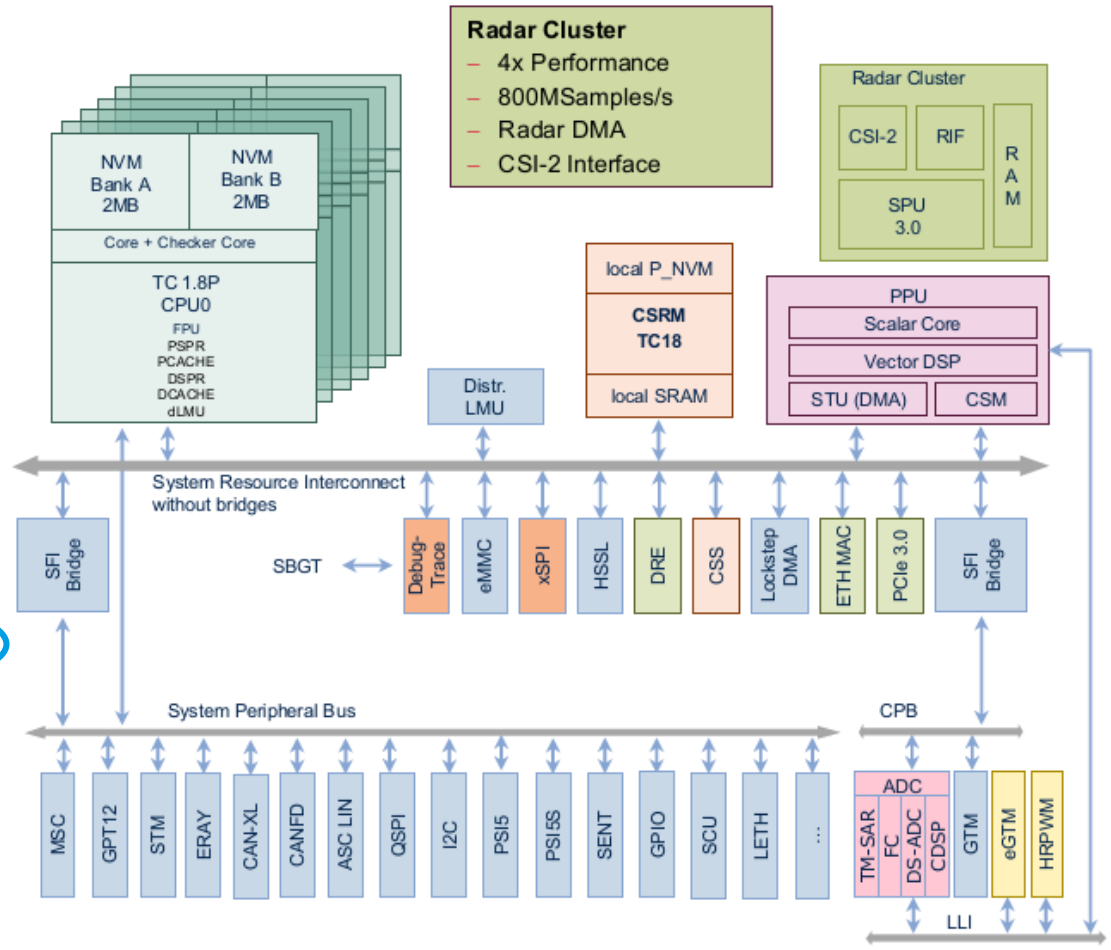
Bigger Tightly Coupled SRAM for increased performance

Full AB-Swap Support

Debug and Trace
Safe and the secure in field

xSPI
External Memory Interface

(i) Note: Quad SPI instead of queued SPI



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

CSRM
New high performance Security Modules with QM 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 and CAN-XL

New communication routing accelerator:
- DRE- Data Routing Engine

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

hitex
EMBEDDED TOOLS & SOLUTIONS

Now we will get a bit more technical

Lead devices (TC4Dx & TC49x) will use eFlash, the other ones will use future proof RRAM NVM

hitex
EMBEDDED TOOLS & SOLUTIONS

› NVM Type  › eFlash  › RRAM NVM

		4 MB	4 + 0,5* MB	6 + 0,5* MB	8 + 0,5* MB	12 + 0,5* MB	16 + 0,5* MB	20 + 1* MB	24 + 1* MB
Cores 6/6 + 1*	500 MHz							TC4Dx PPU 256b	TC4Zx
Cores 5/5 + 1*	400 MHz							TC49x PPU 256b	
Cores 4/4 + 1*	400 MHz					TC46x PPU 256b	TC48x		
Cores 3/3 + 1*	400 MHz				TC4Ex PPU 128b				
					TC44x				
Cores 2/2 + 1*	400 MHz	TC45x PPU 256b		TC4Px PPU 128b					
				TC42x					
Cores 1/1 + 1*	400 MHz		TC4Sx						
TriCore/LS +CSRM									

TC4x enhancements

Performance increase
Up to 500 MHz

Parallel Processing Unit (PPU)
to drive further innovation like virtual sensors and MPC**

Cutting edge security features
to protect with future Post-Quantum Cryptography, ISO/SAE 21434 certified process

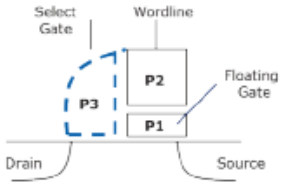
Hypervisor to combine many applications on one MCU and to enable SW-sharing on one Core with ensured FFI**

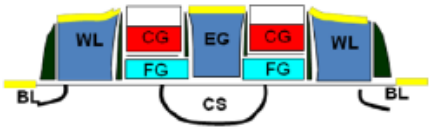
Next Level of Communication
up to 5 Gbit/s ETH,PCI Express

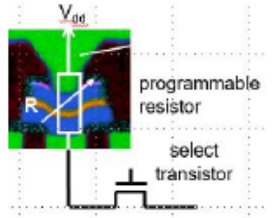
Model-based SW development
TC4x Hardware-Support-package

**Model Predictive Control, FFI = Freedom For Interference

RRAM vs. eFlash



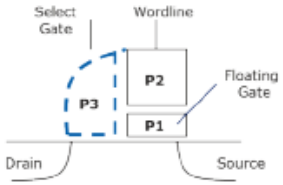


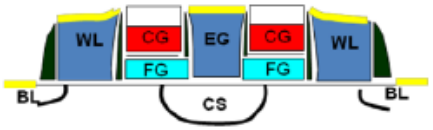


	Flash 40nm	Flash 28nm	RRAM-NVM 28nm
Access Code NVM	30ns	15ns	20ns
Access Data NVM	100ns	50ns	50ns
Write Code NVM	1.1MB/s 1k content updates 20y retention 16kB sector protection	2MB/s 1k content updates 20y retention 16kB sector protection	0.5 MB/s up to 3MB/s device dependent 1k content updates 20y retention 16kB sector protection
Erase	2MB/s @ 16kB granularity	2MB/s @ 16kB granularity	no erase needed
Write Data NVM *w/o Erase time	75µs*/8Byte 125k updates / 10y retention	150µs*/8Byte 250k updates / 18y retention	100µs/8Byte 250k updates /20y retention
Cycle performence (erase+write)	0.75MB/s	1.2 MB/s	0.5 MB/s up to 3MB/s device dependent
Supported grade	up to grade 0	up to grade 0	target extended grade 1, T_{jmax} 160°C
EE emulation	complex algo	complex algo	just write, no erase, no disturb
Parallel module operation	read yes, no for write and erase	read yes, no for write and erase	yes including parllel write on all modules

RRAM vs. eFlash

(i) Note: faster write access for e.g. error logs and less complexity (fewer steps to follow)





	Flash 40nm	Flash 28nm	RRAM-NVM 28nm
Access Code NVM	30ns	15ns	20ns
Access Data NVM	100ns	50ns	50ns
Write Code NVM	1.1MB/s 1k content updates 20y retention 16kB sector protection	2MB/s 1k content updates 20y retention 16kB sector protection	0.5 MB/s up to 3MB/s device dependent 1k content updates 20y retention 16kB sector protection
Erase	2MB/s @ 16kB granularity	2MB/s @ 16kB granularity	no erase needed
Write Data NVM *w/o Erase time	75µs*/8Byte 125k updates / 10y retention	150µs*/8Byte 250k updates / 18y retention	100µs/8Byte 250k updates /20y retention
Cycle performence (erase+write)	0.75MB/s	1.2 MB/s	0.5 MB/s up to 3MB/s device dependent
Supported grade	up to grade 0	up to grade 0	target extended grade 1, T_{jmax} 160°C
EE emulation	complex algo	complex algo	just write, no erase, no disturb
Parallel module operation	read yes, no for write and erase	read yes, no for write and erase	yes including parllel write on all modules

ADC improvements

AURIX™ ADC

(i) Note: dedicated DSP integrated for ADC-block
→ not all sample data needs to be transmitted via bus
→ lower bus load

TC2xx
Technology: C65

9 x DSADC SNR 80dB
11 x VADCs 1Msps 12bit
SPB 100MHz

TC3xx
Technology: C40

14 x EDSADC SNR 80dB
12 x EVADCs 2Msps 12bit
8 x FCC 5Msps
SPB 100MHz

TC4xx
Technology: C28

14 x DSADC **SNR 86dB**
4 x EXMOD (8x for B-step)
12 x TMADCs 4Msps 12bit
10 x "really fast" FCC 50Msps
18 x CDSP
CPB 200MHz

(i) Note: simultaneous sampling + digital filter directly attached

(i) Note: CDSP via separate toolchain (or libraries)

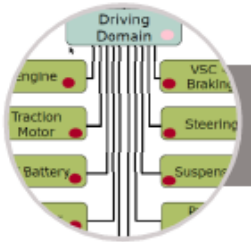
There is a demand for higher degree of isolation
Answer: TC4x with Hypervisor Mode

hitex
EMBEDDED TOOLS & SOLUTIONS

Isolation

- Isolation containers are called VM; Requirements starts from 1 - 2 VMs per core up to 30 VM for a single ECU
- A VM isolates application (SW Unit) execution and control paths
- Isolation has to be safe, secure and easy to use

Use cases



Consolidation (Fusion)

- Combine several apps on one HW
  - to **reduce number of ECUs**
  - to efficiently use the computing power
  - Agile SW development with **split SW units** (teams/organizations)
- Combining applications with different OS on one MCU

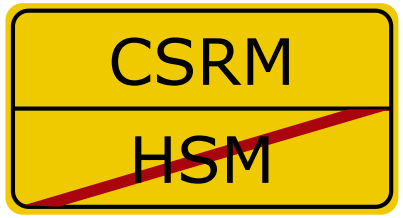
Separation (Fission)

- Split existing monolithic apps due to
  - Safety (separation of ASIL levels)
  - Security
  - Liability (separate SW from partners or legislation compliance)
  - SW dev. flexibility (enable exchange of parts and collaborative development)

Flexibility (New features)

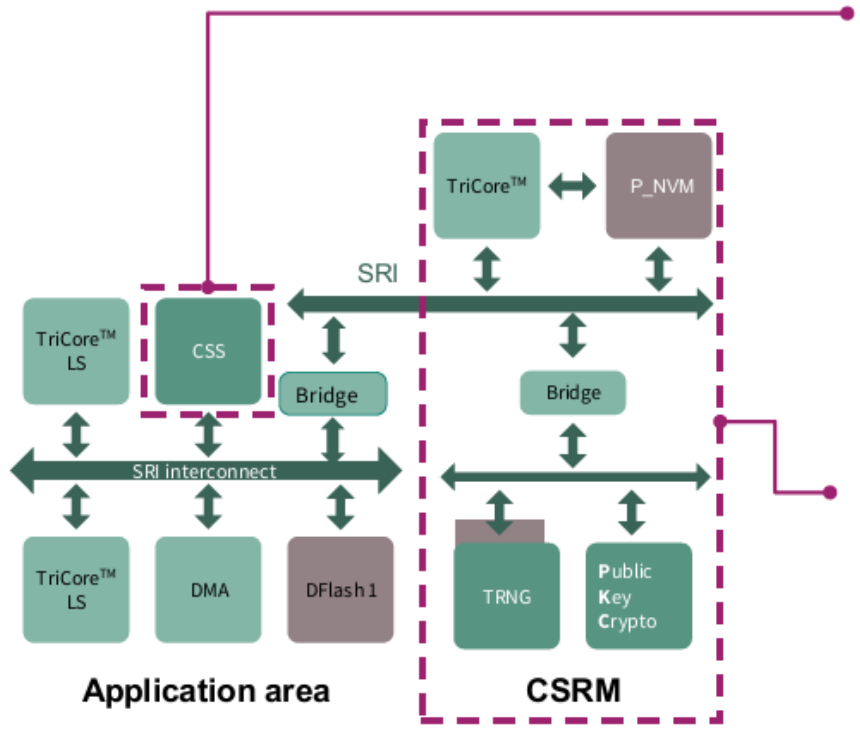
- Separate startup and shutdown of a VM app
- Independent exchange („reprogram“) of a VM (e.g. over the air update)
- Flexible activation and deactivation of features

Security



hitex
EMBEDDED TOOLS & SOLUTIONS

New AURIX™ TC4x security cluster



High performance security with high throughput will be a key requirement for future Chassis applications

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

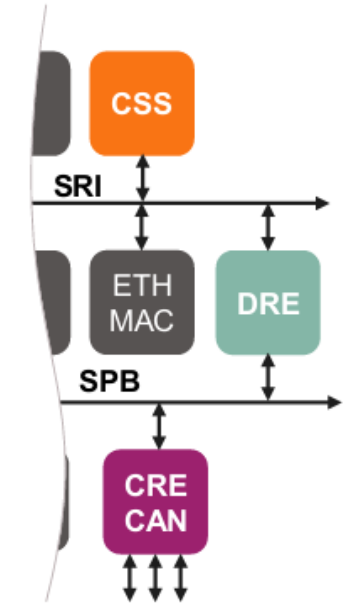
Cyber security real-time module (CSRM) for performance increase

- Upgrade to TriCore™ 1.8
  - providing ~5-15x more performance vs. ARM M3 in TC3x HSM
- CSRM as trusted secure HW environment supporting new security standards (e.g. ISO 21434)
- Private P_NVM within CSRM which supports individual security SW updates independent of application core
- Enables realization of multiple security use cases for wide ranging applications

(i) Note: CSS also raises SMU

New routing accelerator effectively reduces communication load on CPUs

Routing accelerators in AURIX™ TC4x



DRE = Data Routing Engine
CRE = CAN Routing Engine
CSS = Cyber Security Satellite

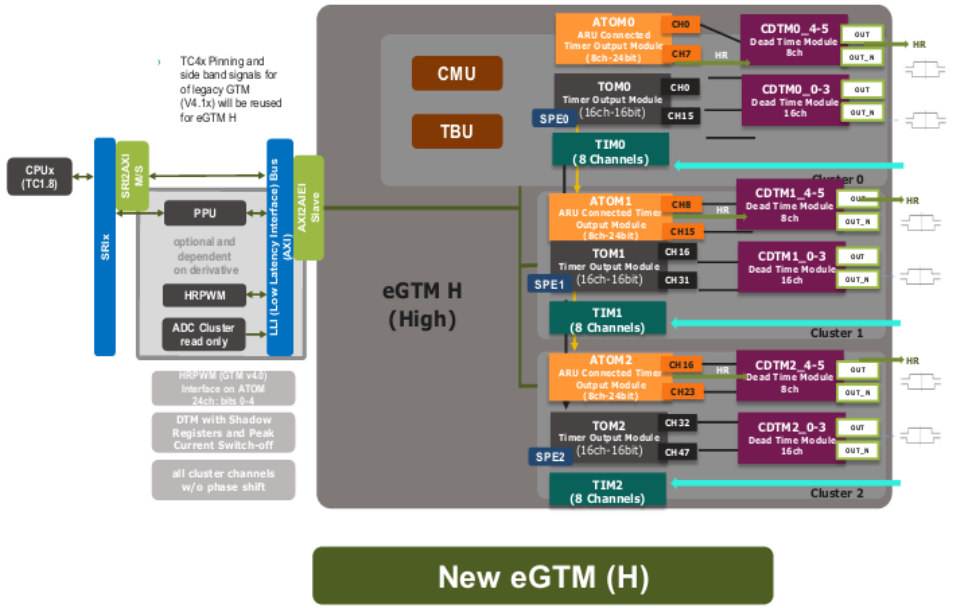
Generation routing functions	– Unicast and Multicast Routing: up to 4 destinations – Round-robin (Non-starving) priority for transfers from source / destination CAN Modules
CAN – CAN routing	– Routing between CAN Interfaces to CAN interfaces – CAN Frame Modifier (only for Unicast Routing) – CAN-ID, CAN Frame Format (Classical or CAN FD), DLC (Length of the CAN Frame)
CAN – Ethernet routing	– Routing of CAN frames to/from Ethernet – IEEE 1722 AVTP ACF frame formatting – Ethernet AVTP ACF Transmit Trigger Modes: single Transmission, Timer Event, Buffer Full Event and Software Trigger
CAN – Memory routing	– Routing of received CAN frame from CAN Interface to a configurable MCU internal memory address – Hardware based address increment and wrap around – CPU Interrupt generation to notify new CAN frames stored in its memory
Safety	– Timeout monitoring: Timestamps appended to Routing frame at Source and its freshness is verified at the Destination – Failure mode: Lost / Unintended or delayed CAN/DRE operation and DRE read/write from/to the wrong DRE source address
Security & Debug	– SecOC Hardware acceleration for Secure CAN frame MAC generation and verification – Routing event record and MACsec support

(i) Note: Automatic routing saves SW execution / CPU load

Enhanced Generic Timer Module (eGTM)

Features details

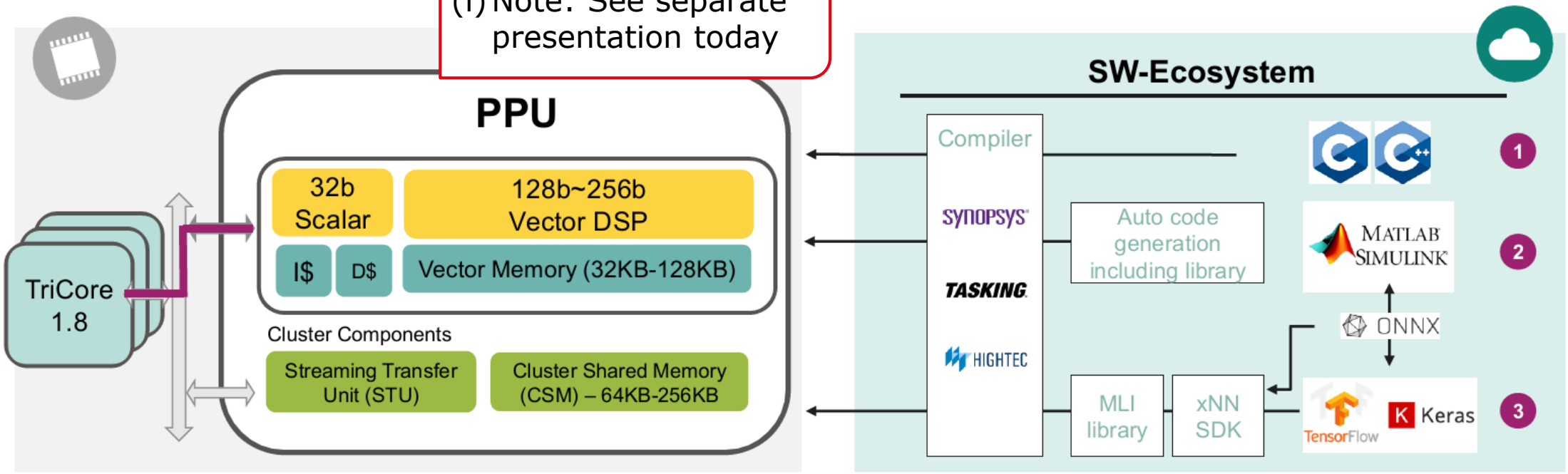
- Created to improve access latency from TriCore™ to legacy GTM
- Speed up to 400MHz TriCore™ CPU frequency
- Connected to new private ADC/Timer Low Latency Interface (LLI) which also operated @ CPU speed
- Synchronization of up to 3 clusters with same clock domain which allows synchronous behavior of up to 24 ATOM ch
- Introduction of a HighResolution PWM (HRPWM) extension allowing up to 24ch (w DTM 48ch) a enhanced resolution from 200MHz (5ns) to 156ps (nominal)



TC4x Parallel Processing Unit (PPU): a scalable SIMD Vector DSP & scalar core with dedicated SW-tool-chain

hitex EMBEDDED TOOLS & SOLUTIONS

(i) Note: See separate presentation today



› **Execution 3x faster** than competitor solutions, **enabling Neural network based** algorithms and **High-speed-control implementations**

› **Unique SW Ecosystem**: Model-based development, connected with latest Machine-learning-tools like Tensor-flow is enabling **easy usage and fast time-to market**

Wrap-up

- TC4x is a significant step up in features and performance
- It is a powerful tool and useful in a variety of applications
- The complexity is not to be underestimated, but valuable design-in support is available via the PDH-program

hitex

AURIX KNOWLEDGE LAB 2024

Any Questions?

ETAS HIGHTEC imagimob An Infineon Technologies Company

infineon pls Development Tools TRUST IN SOFT