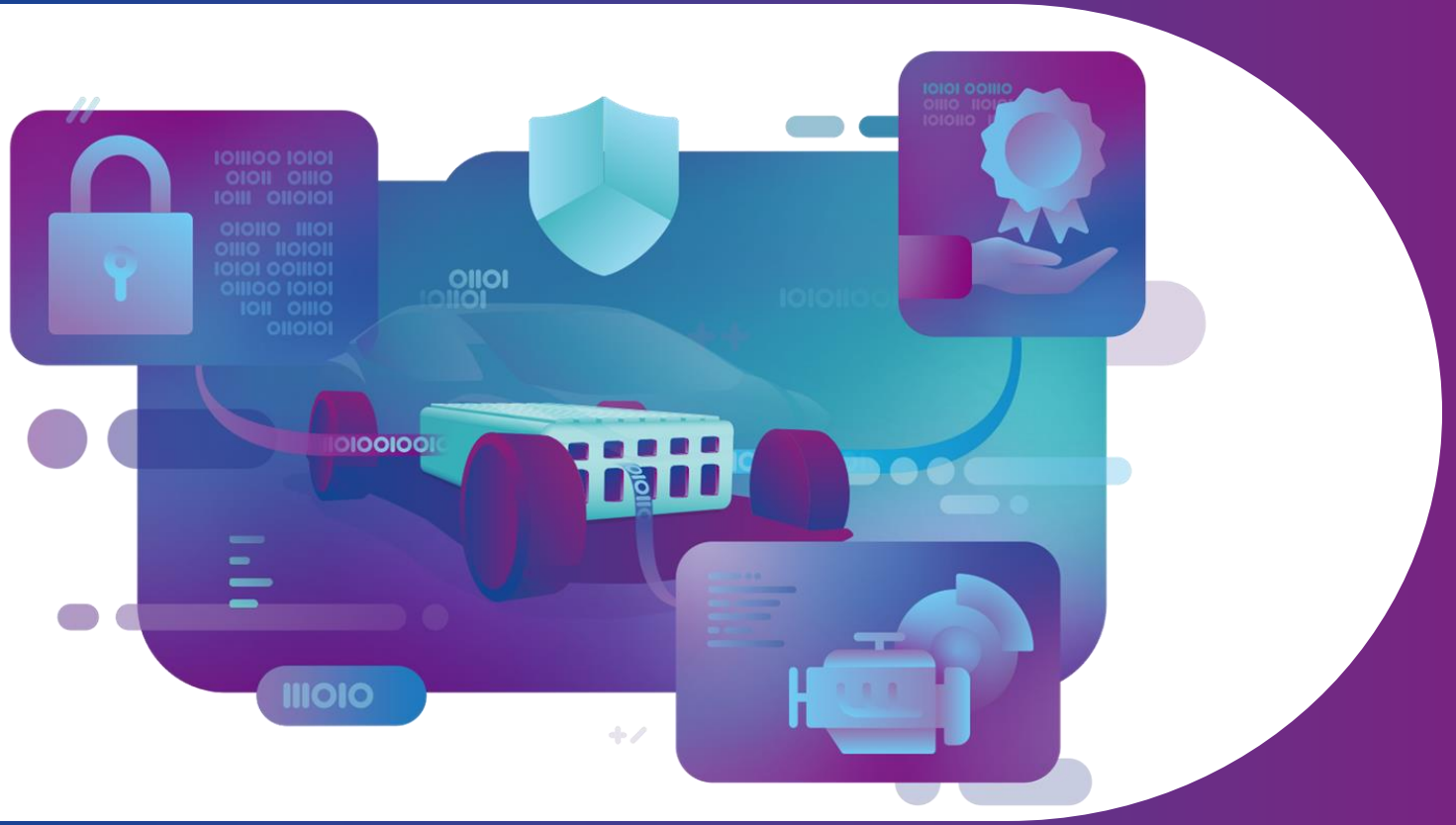
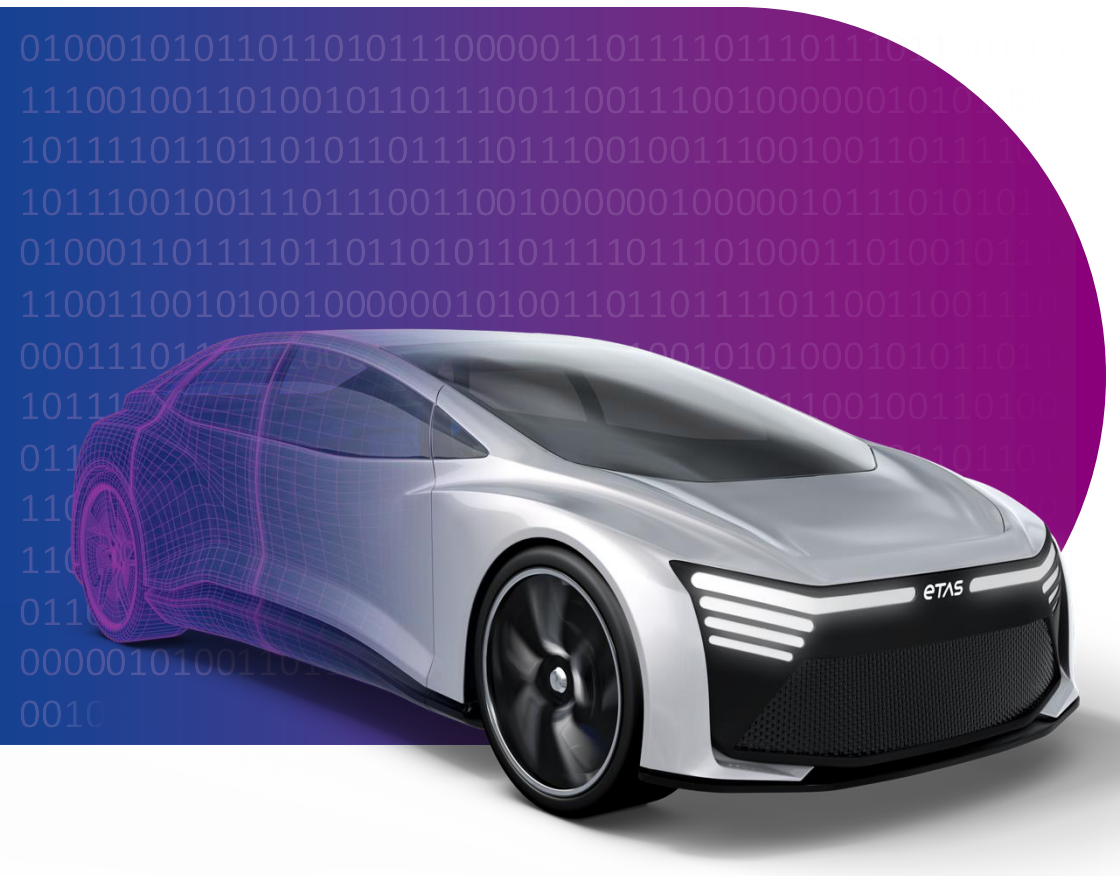


Safety, Security and the Future of **Embedded Mobility**

Janak Patel
September 2025

Welcome to ETAS

Enabling the future of software-defined vehicles



Software is playing an increasingly important role in automobiles. It defines the vehicles' functionality and performance.

The vision is the truly **software-defined vehicle** that is fully programmable and brings extra capacity for future software improvements.

Furthermore, software provides safety, comfort, and driving characteristics, and offers added value to the user.

With solutions for software development, operation, and cybersecurity, **ETAS** enables its customers to build the best software in and outside the vehicle.

Automotive Transformation – Customer Experience

A transformation from an isolated mechanical car to a highly inter-connected software-driven car for ultimate customer driving experience:

Electrification

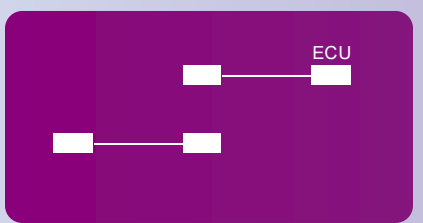
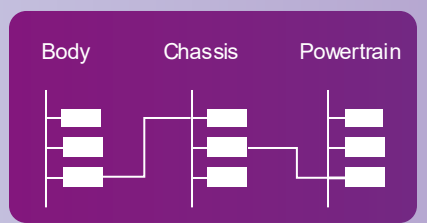
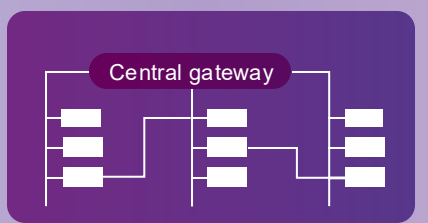
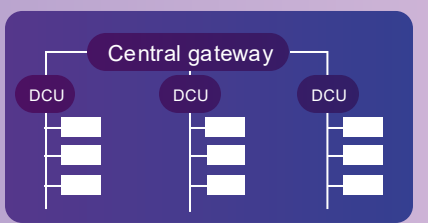
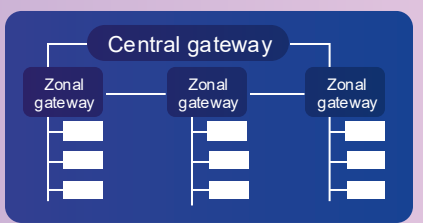
Automated Driving

Digital User Experience

ADAS is at the core of the automotive transformation to bring safety, efficiency, long-term value, sustainability and much more.

Automotive Transformation – System Architectures

Separate Sense/Actuation from Logic

Distributed E/E Architecture			Domain centralized	Vehicle centralized
				
– Independent ECUs – Isolated functions – Simple and basic ECU – Each Function has its own ECU (One function – one Box)	– ECUs grouped based on application – Collaborations of ECUs within the same domain – 3 or 4 independent networks	– Central gateway – Stronger collaborations of ECUs – Cross-functional connection – Ability to handle complex functions	– Domain Control Units – Stronger consolidation of functions – Over-the-air updates capabilities	– High-performance compute unit – Physical location-based ECUs – Ethernet backbone – SW decoupled from HW
Yesterday		Today		Tomorrow

E/E architectural transformation is at the heart of the software-defined vehicle, laying the foundation for ADAS/AD, connectivity, infotainment, and digital cockpit applications.

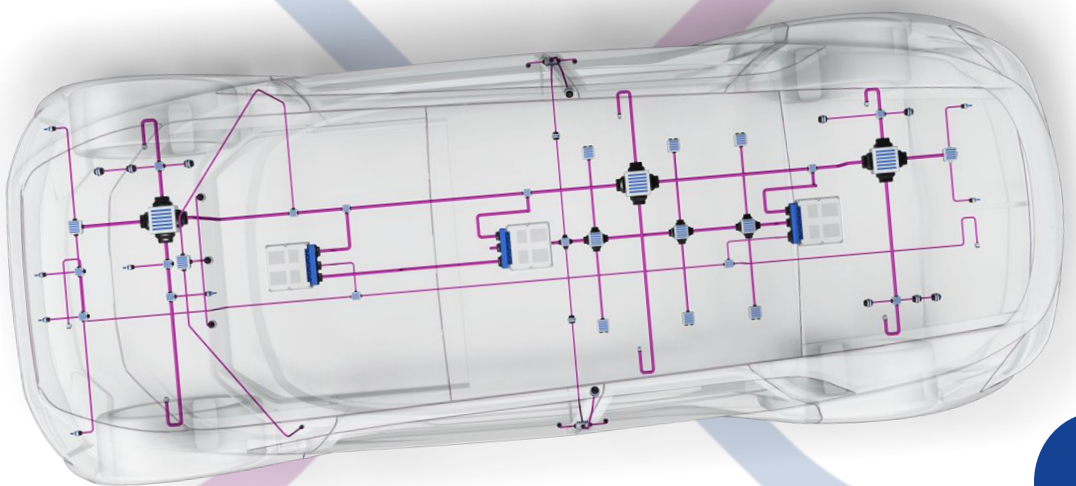
Software-defined vehicle (SDV)

Value & benefits

Establish feedback loop

Establish new business models

Enhance end-to-end security



Enable preventative maintenance

Increase automation

Continuously Innovate

Enhance customers' experience

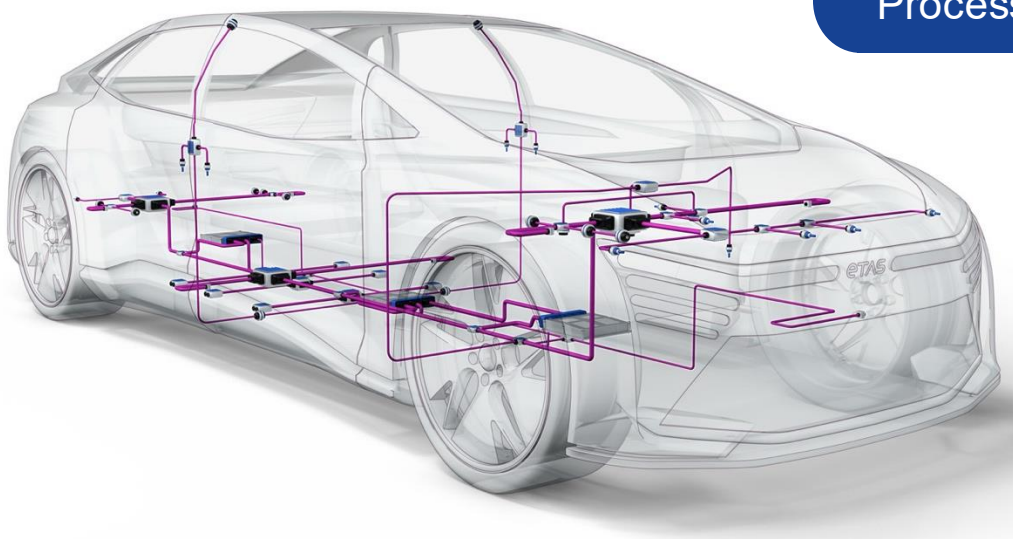
Vehicle Computer

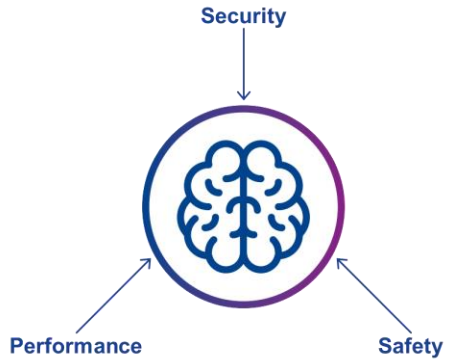
at a glance

Flexibility

Intelligence

Processing power





Optimize vehicle's performance and operation

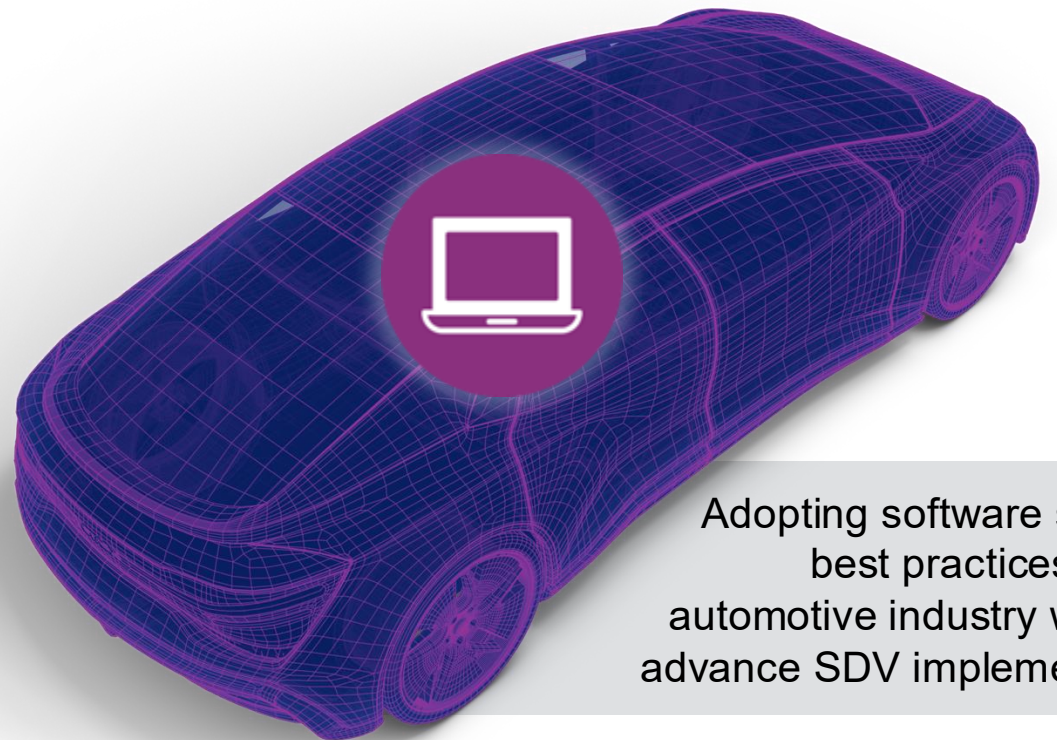
A vehicle computer is a system that collects and processes complex and high bandwidth data from different ECUs, and sensors in the vehicle, such as ADAS, infotainment, navigation and powertrain applications.

Most of these vehicle computers need system-on-chip (SoC) to compute the large set of data and provide results.

Connected Vehicles

Vehicle computer & security

- Constant connectivity
- Authorization and access management
- Third-party software ecosystem
- Speed of software delivery
- Continuous updates



Adopting software security best practices by the automotive industry will help advance SDV implementation

Challenges

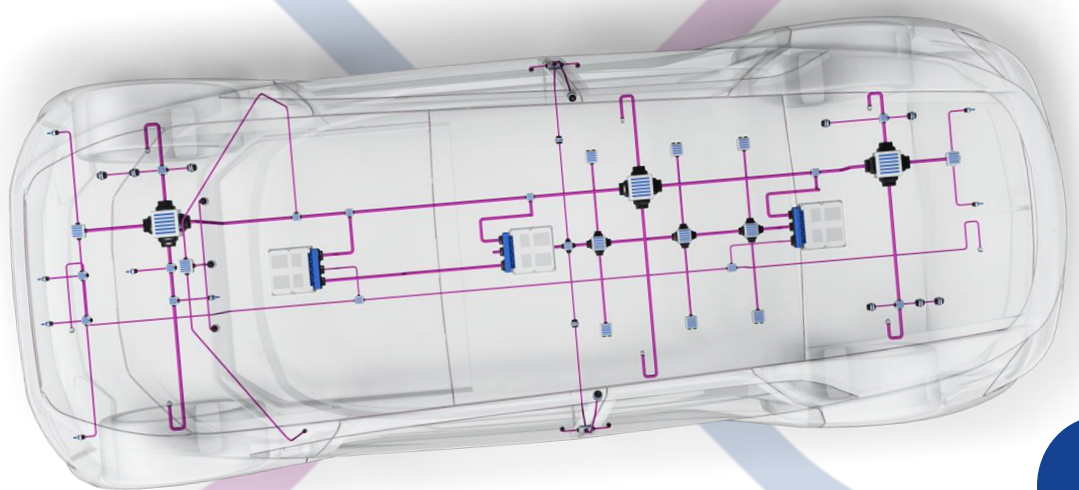
Software-defined vehicle (SDV)

Some challenges

Domain specific ECUs still required

Programming models need to evolve

Functional safety



Still have hardware first mentality

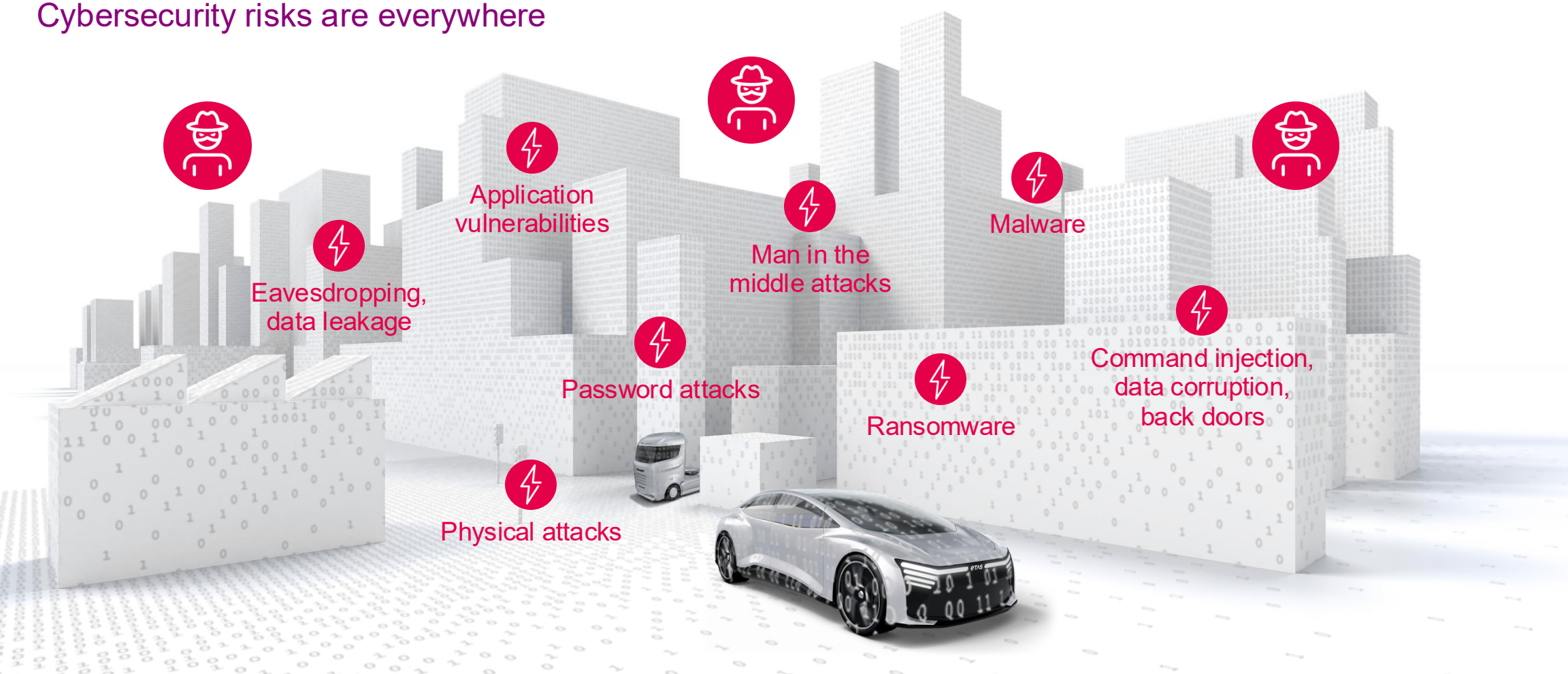
Lack of standardization

Change cascading

System level SW architecture missing

Macro Level Challenges

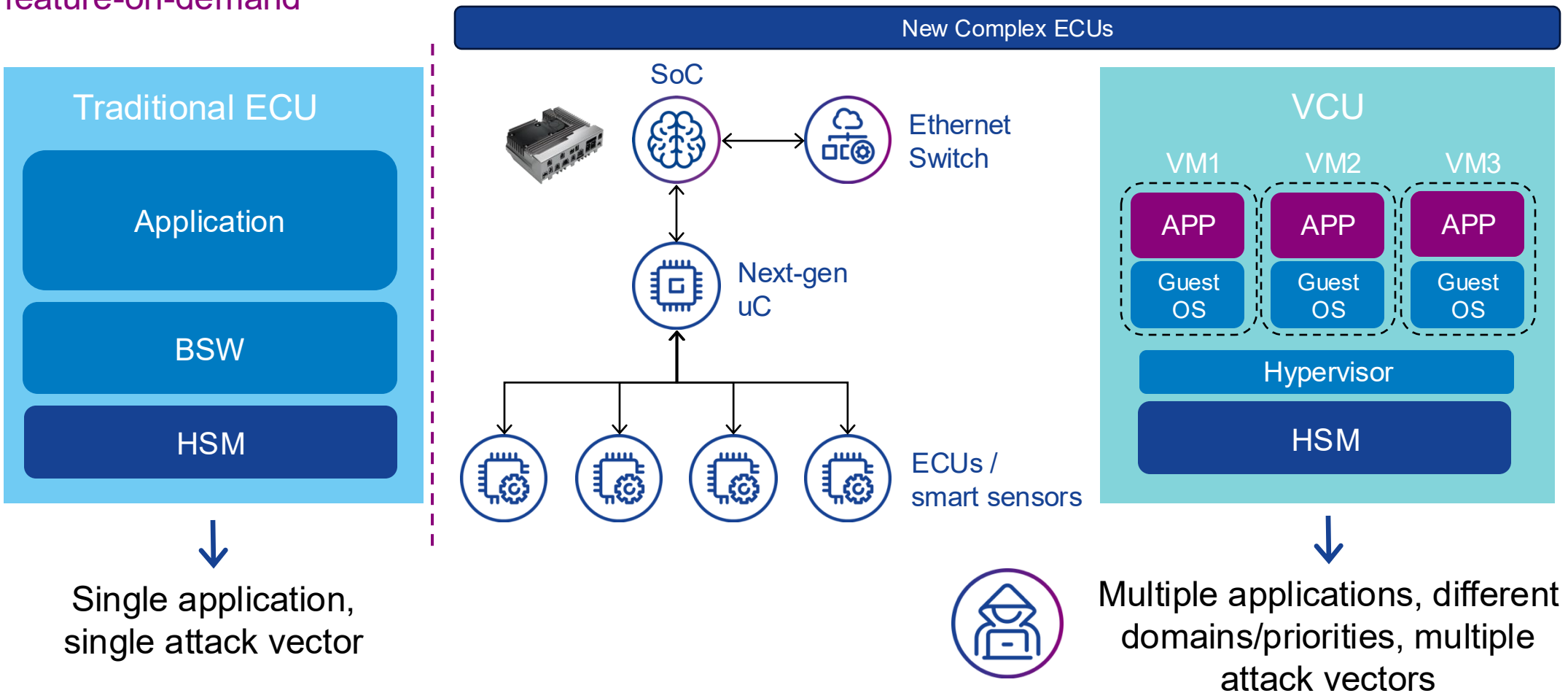
Cybersecurity risks are everywhere



High complexity and connectivity are increasing the attack surface.
All connected endpoints and critical infrastructure of the ecosystem must be protected.

Challenges in Complex Electronic Control Unit (ECU)

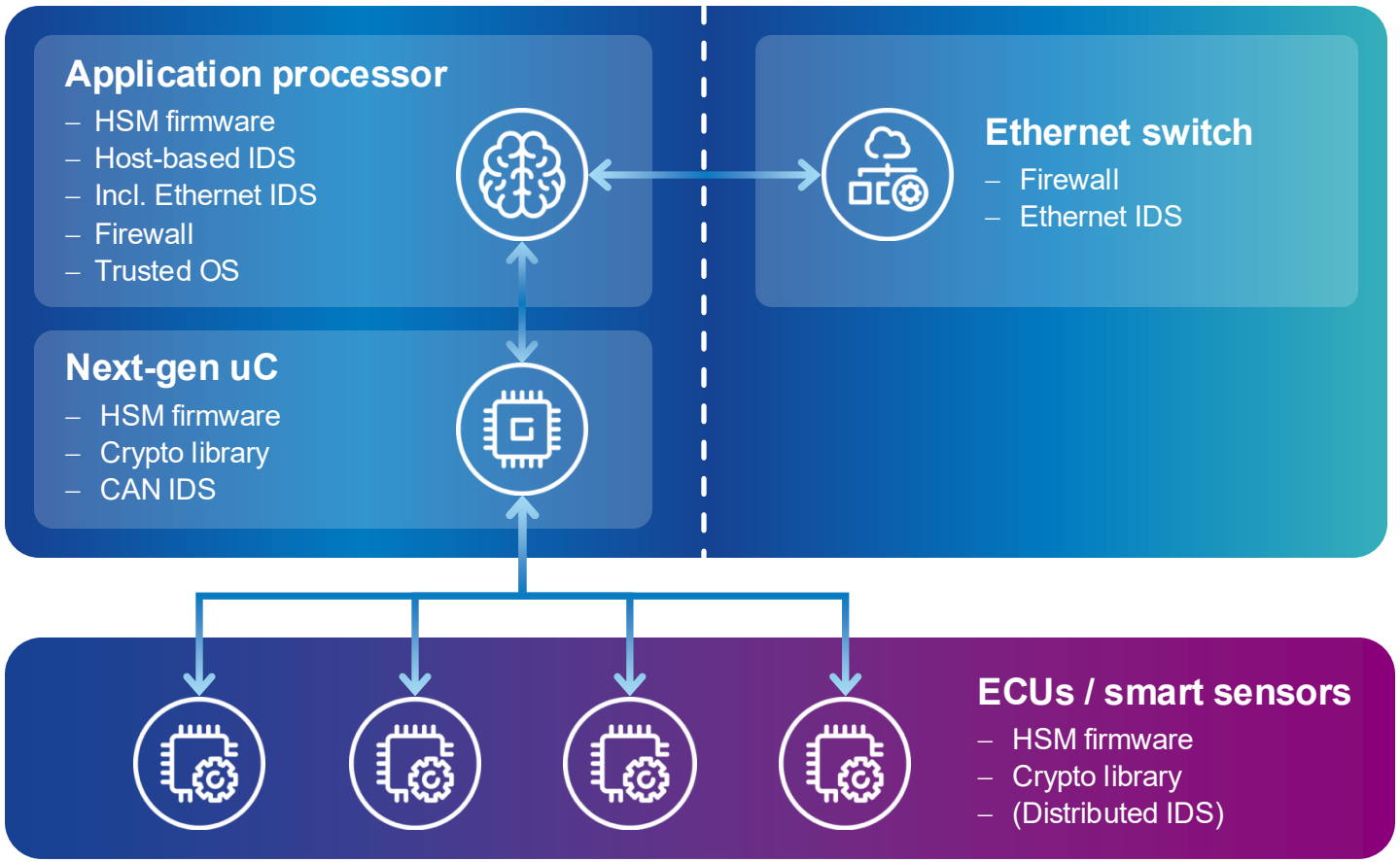
Evolving functionality and features, shifting threats: navigating the evolving attack landscape of feature-on-demand



Security Solution

Vehicle Computer Security

What are the security components for different ECUs?



Cybersecurity Strategy

Layered defense

- Be able to react on different levels: adequate local response
- Avoid single points of failure

Strong isolation of components

- Segment the system into specialized domains
- Restricted and secure inter-domain communications

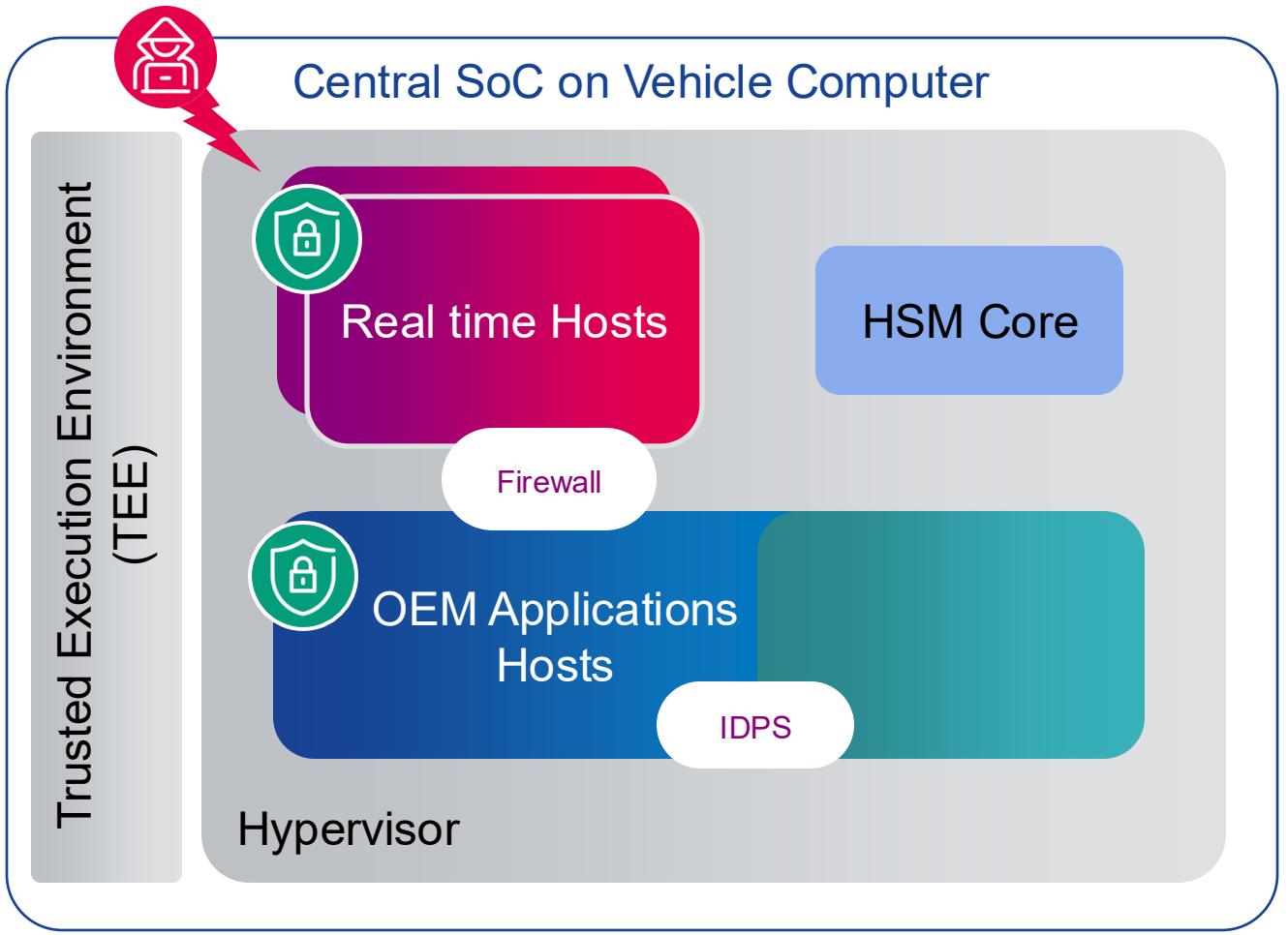
Local security response

- Automatic security response on the device
- Essential functions stay operational during incidents

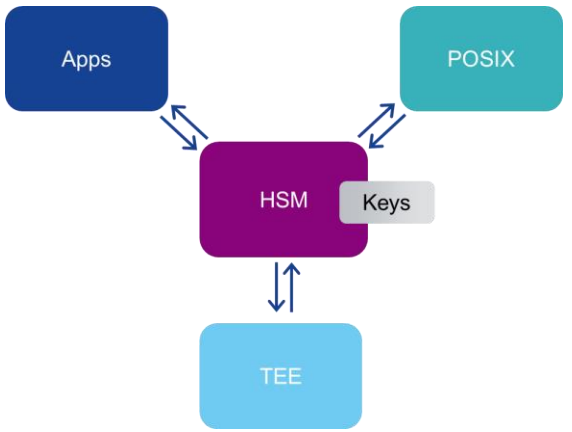
Centralized monitoring and dynamic prevention

- Utilize a core security domain
- Detect anomalies and activate adaptive countermeasures across domains in real time

Mitigating Risks Effectively



- Secure the different domains (multi-tenants) within the VCU
- Employ zero-trust concept
- Minimize impact on user experience



Leveraging Security Components

Key security pillars of vehicle computer

Trusted Execution Environment (TEE)

- Identify requesting service within a VM (IDS)
- Policy enforcement
- Authentication
- Data integrity
- Confidentiality
- Strong multi-user capability

Hardware Security Module (HSM)

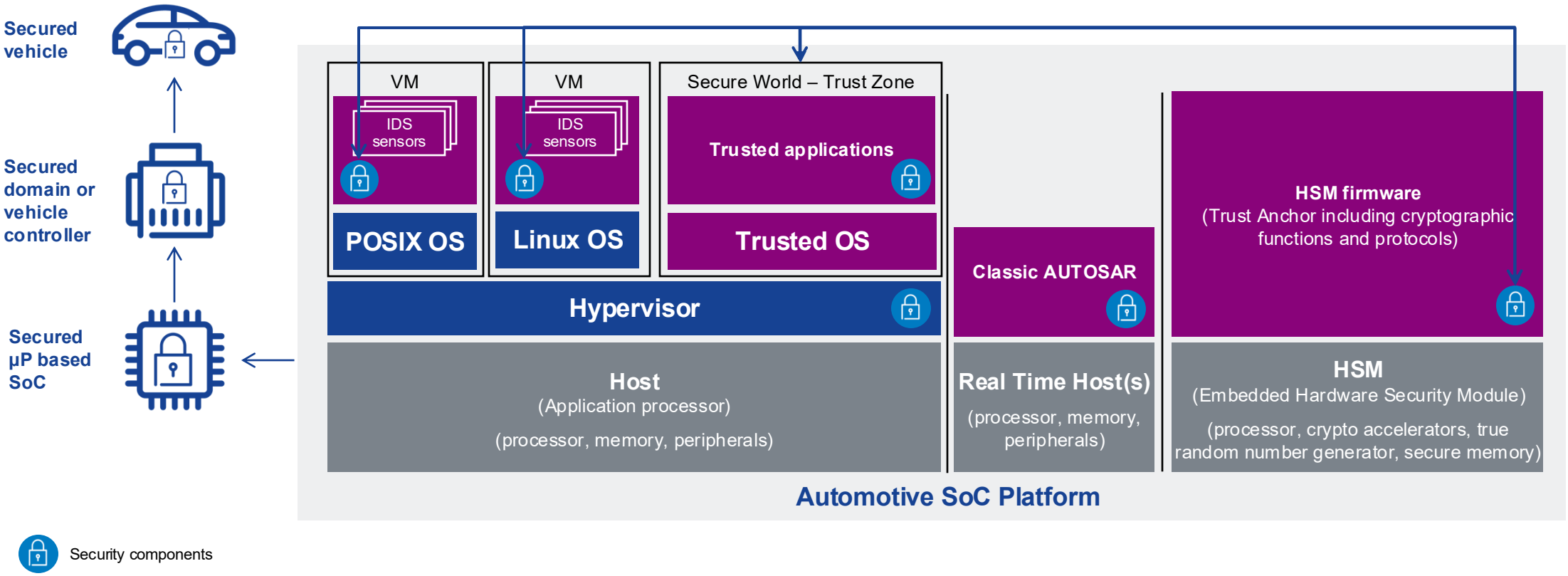
- Root of trust
- Tamper-resistant
- RTMD
- Key storage and encryption, securing critical assets
- Low latency
- Full parallel operation

Intrusion Detection and Prevention System

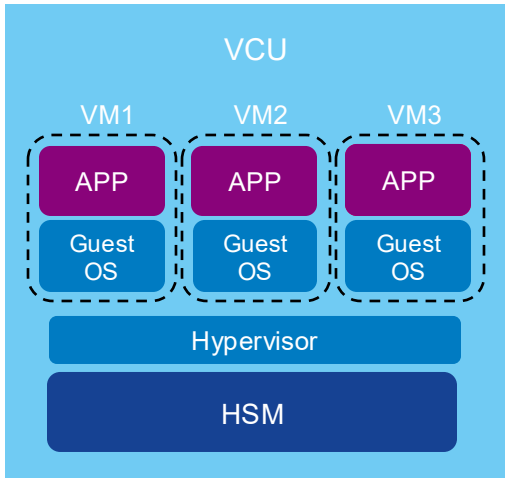
- Multiple IDS sensors can be deployed in a vehicle
- Host-based IDS for single ECU
- Network-based IDS for network traffic
- Firewall management

Securing The Vehicle Computer

Automotive System-on-Chip (SoC) security



Security Flow of ADAS Sensor Messages



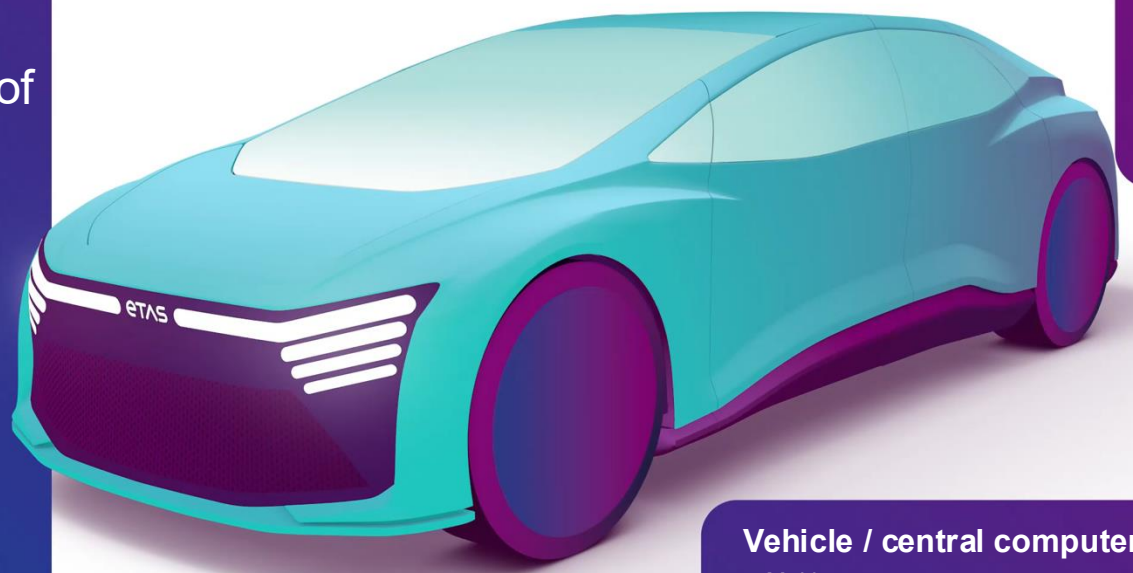
Security implementation needs to consider the high throughput of ADAS sensors to avoid any propagation delay

ETAS Vehicle Computer Security

The de-facto standard for µP based SoC

ETAS CycurSoC, Trusted OS & CycurIDS provide all security functionality of the SoC platform

- Secure boot
- Secure communication
- Secure software update
- Secure diagnostics
- Secure production
- Secure access
- Secure logging
- Intrusion detection and monitoring



Establishes root of trust

Enables system authenticity & integrity

Vehicle / central computer

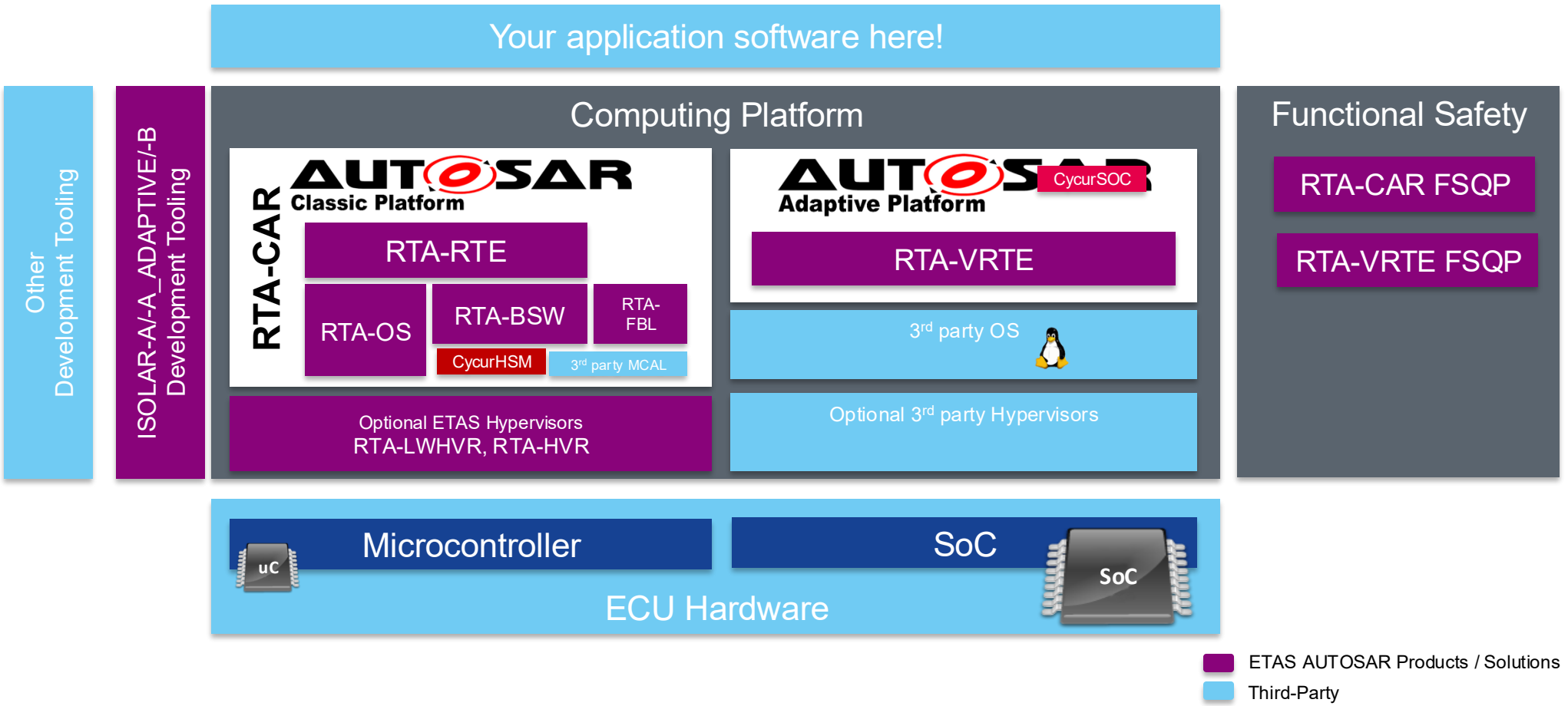
- Multi tenancy
- POSIX OS/Adaptive AR
- Applications in virtual machines
- TEE or HSM based trust anchor

High performance data processing function specific ECU

- ADAS and its connected sensors…

ETAS Solutions

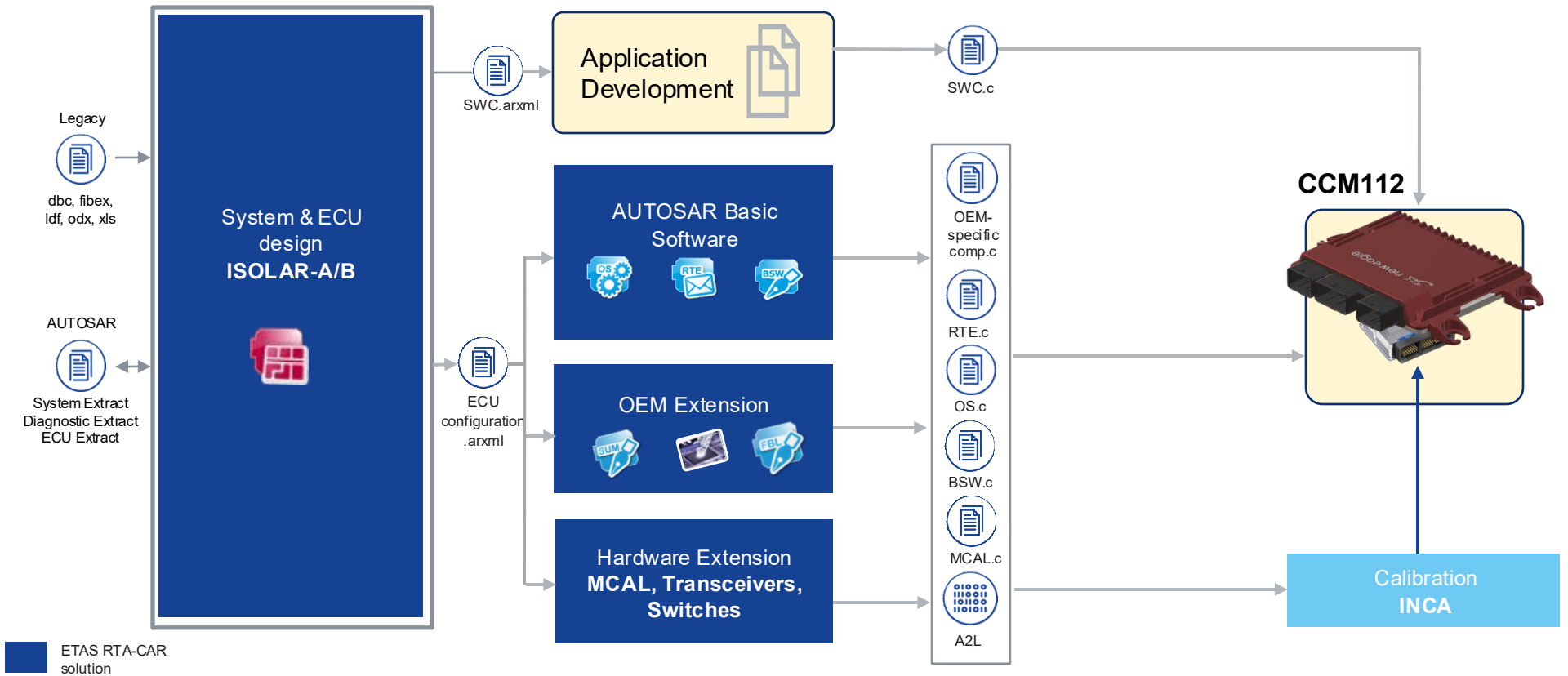
AUTOSAR Classic – safety and security integration



ETAS Solutions

RTA-CAR portfolio overview

In partnership with new eagle TAKE CONTROL



Consulting and Engineering Services: Training, coaching, development and integration, on-site support

New Eagle cooperation

CCM112 with advanced cybersecurity functions powered by ETAS

In partnership with new eagle TAKE CONTROL

- Available on CCM112 in Q4 2025
- Initial feature set will focus on run-time cryptographic services for SecOc and J1939-91C
- Secure boot functionality available in H1 2026
- Makes full use of hardware security module of TC3XX MCU

CCM112

Q & A