# AUTOSAR introduction, Cybersecurity activities and AUTOSAR Opening Strategy

Masahiro Goto, AUTOSAR regional spokesperson Japan

Global Platform Vehicle Cybersecurity Forum

September 14th 2023

Tokyo

# Agenda

- Introduction to AUTOSAR
- Overview over AUTOSAR Security Features
- AUTOSAR Opening Strategy
- Current AUTOSAR/Global Platform collaboration status

# AUTOSAR Mission

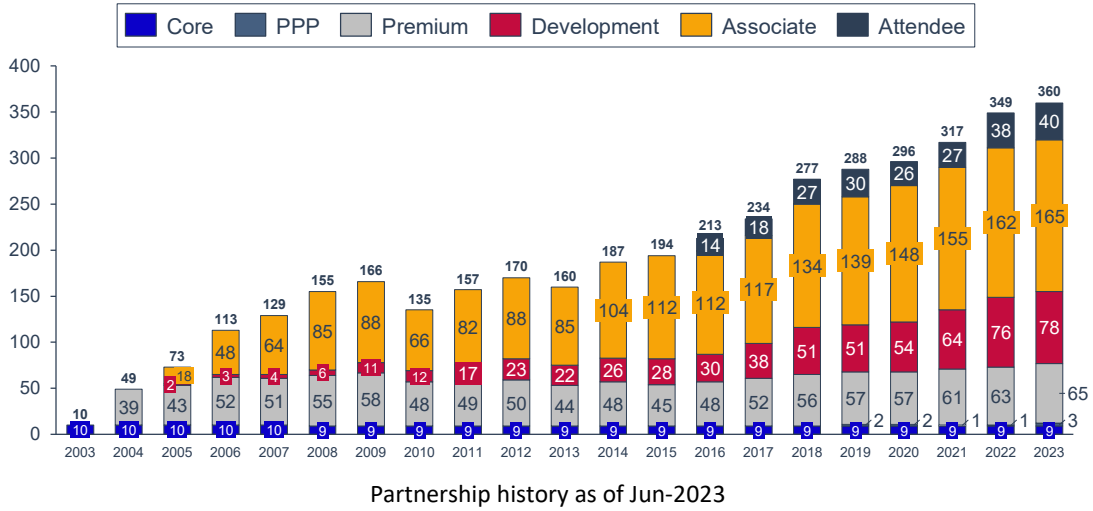
AUTOSAR is a global partnership of leading companies in the automotive and software industry to develop and establish the **standardized software framework** and **open E/E system architecture** for intelligent mobility.

***„If a company develops alone it will be one proprietary solution,***
***if it is shared and used by several partners it becomes technology, and***
***with broad standardization it becomes state of the art and alleviates certification.“***

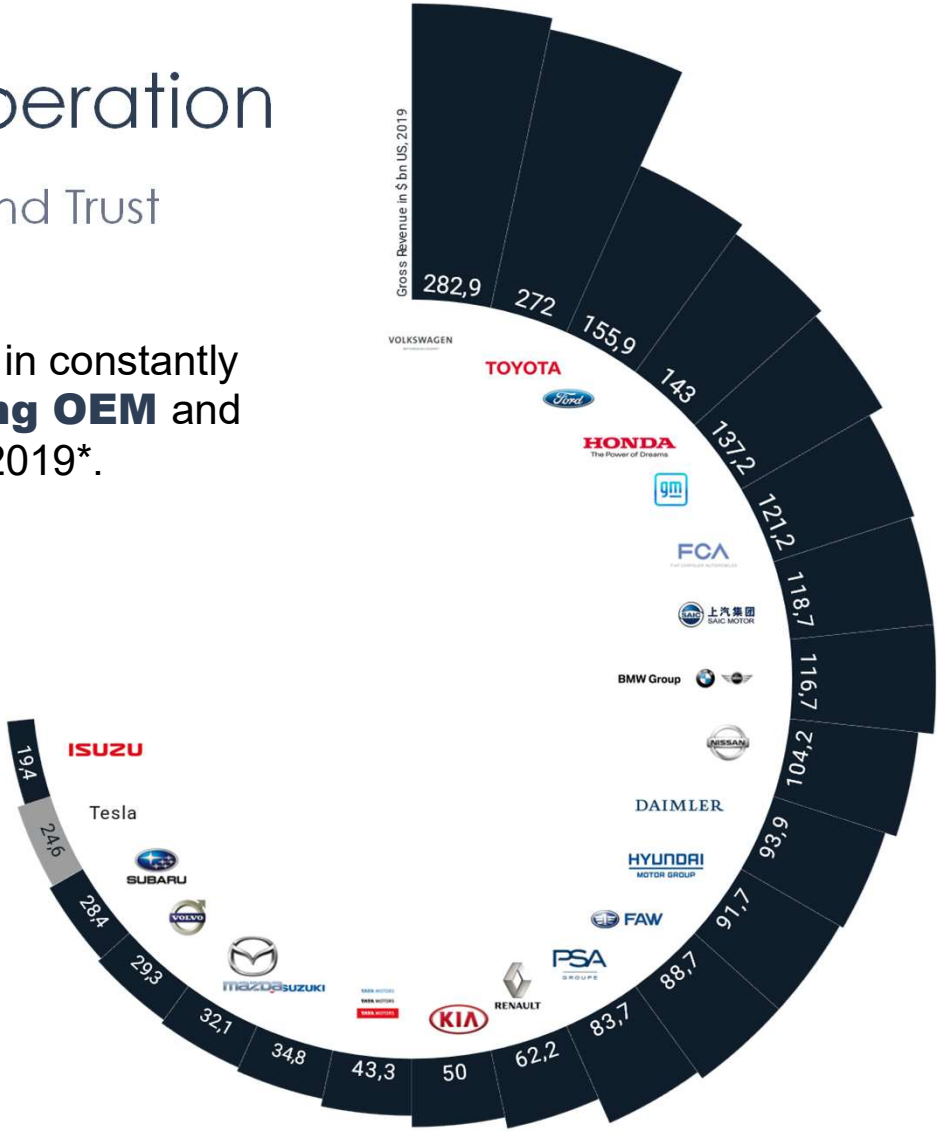
# AUTOSAR Development Cooperation

## A Global Community based on Responsibility and Trust

31 international automotive OEM are AUTOSAR partners in constantly **growing community**. **21** are **under the 22 top-selling OEM** and covering **over 80%** of the **total market revenue** in 2019*.

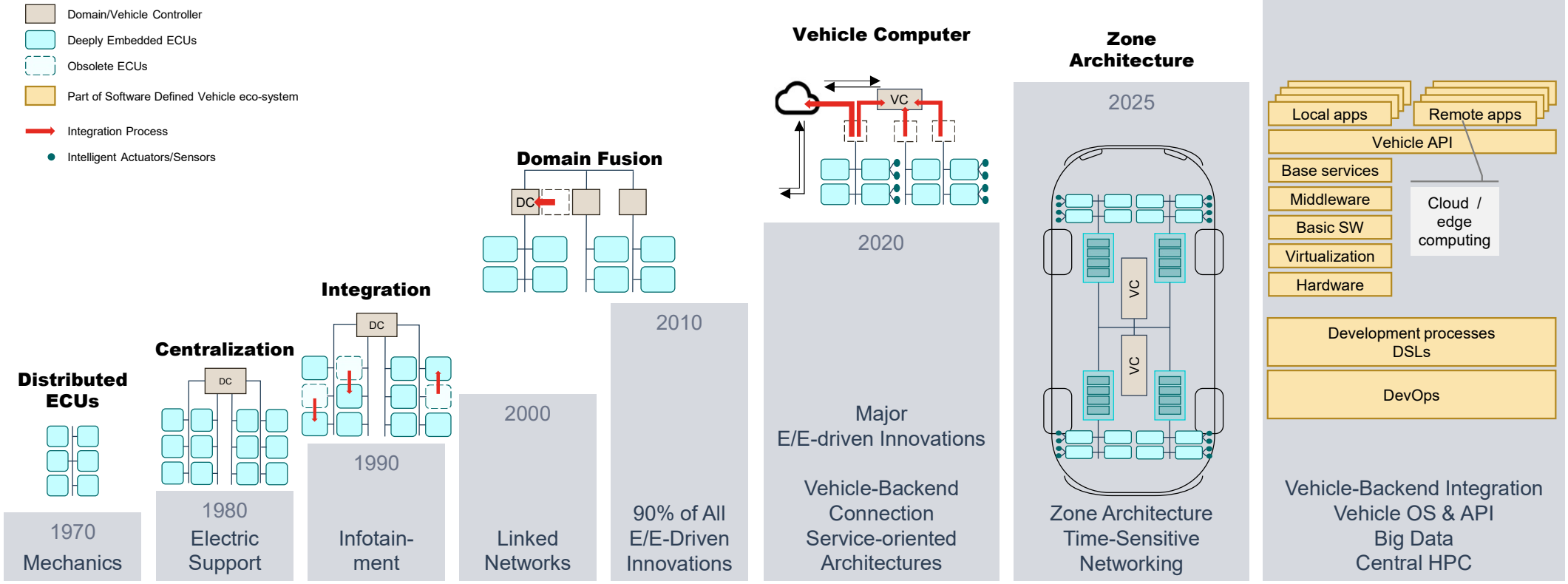



Partnership history as of Jun-2023

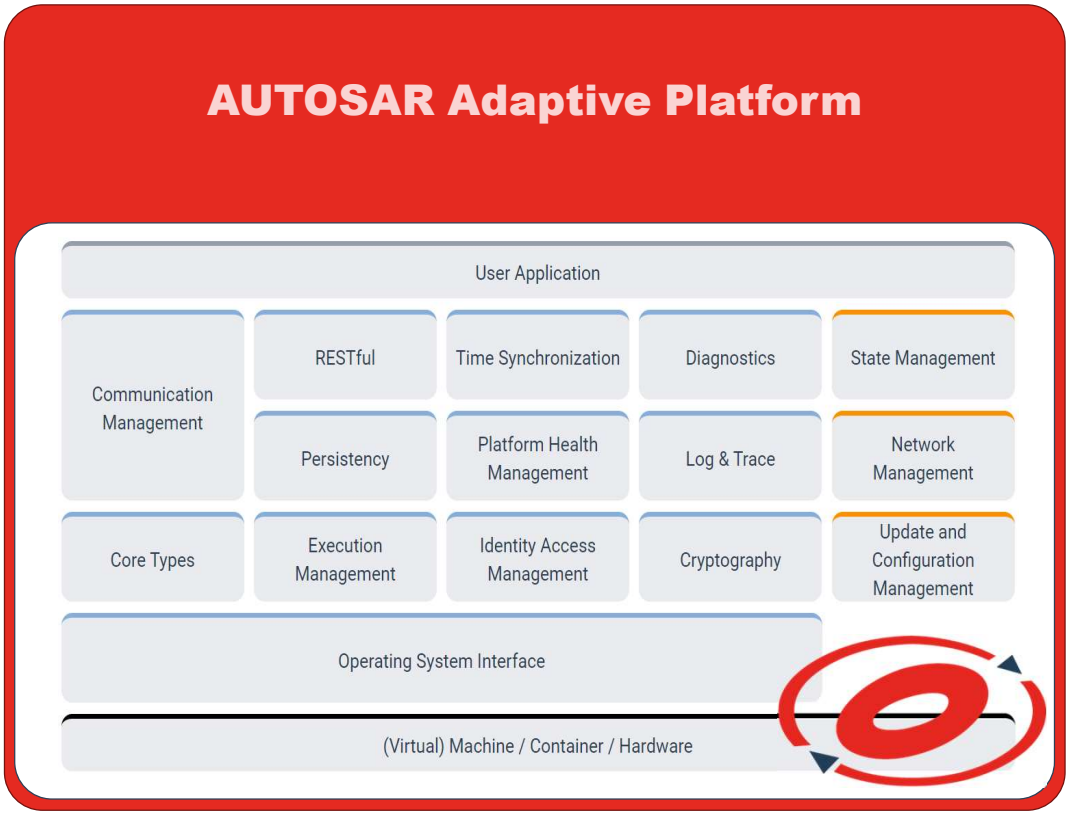


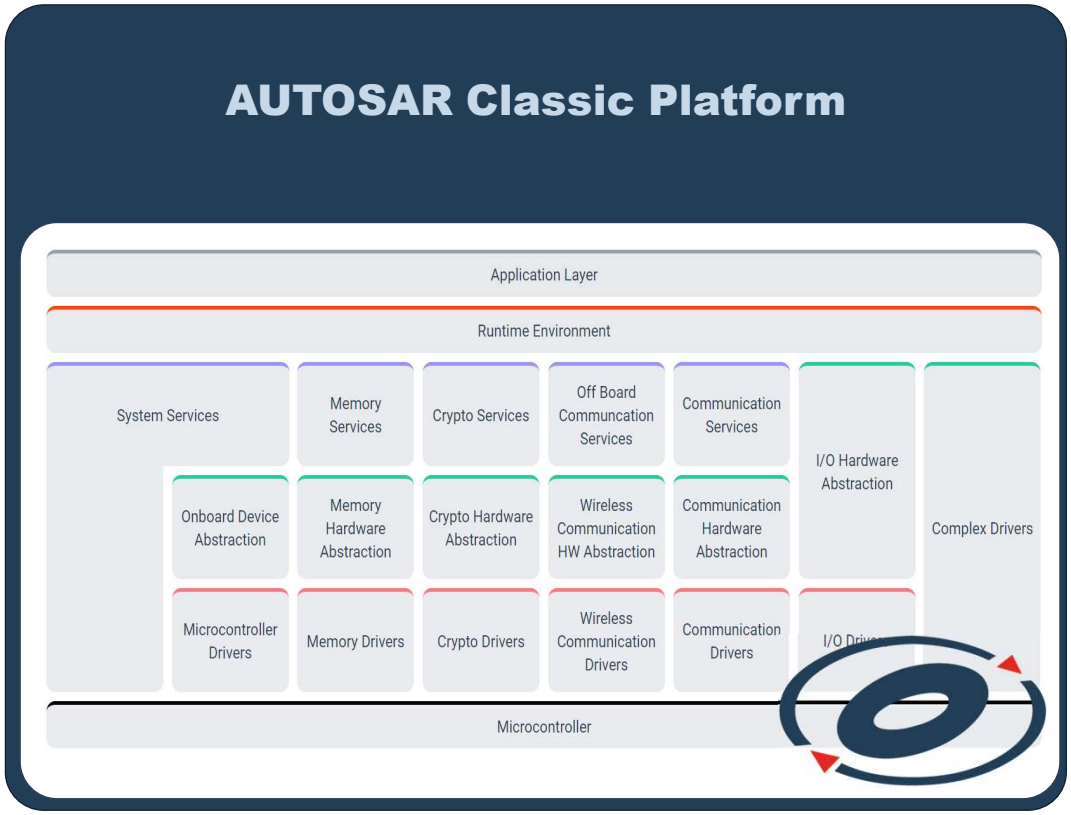

*ref. to The 2019 Strategy&Digital Auto Report, strategy& - part of the PwC network

# Driving changes in E/E architecture



# AUTOSAR Platforms



# AUTOSAR Adaptive and Classic Platform

## What Are the Differences?

| | Adaptive  | Classic  |
|---|---|---|
| Real Time Requirements | **Mid**, in the range of milli-seconds | **High**, in the range of micro-seconds |
| Safety Criticality | **High**, at least ASIL-B | **High**, up to ASIL-D |
| Computing Power | **High**, > 20.000 DMIPs | **Low**, ~ 1000 DMIPs |

# Overview over AUTOSAR Security Features

## Layered Automotive Security Approach

**E/E architecture**

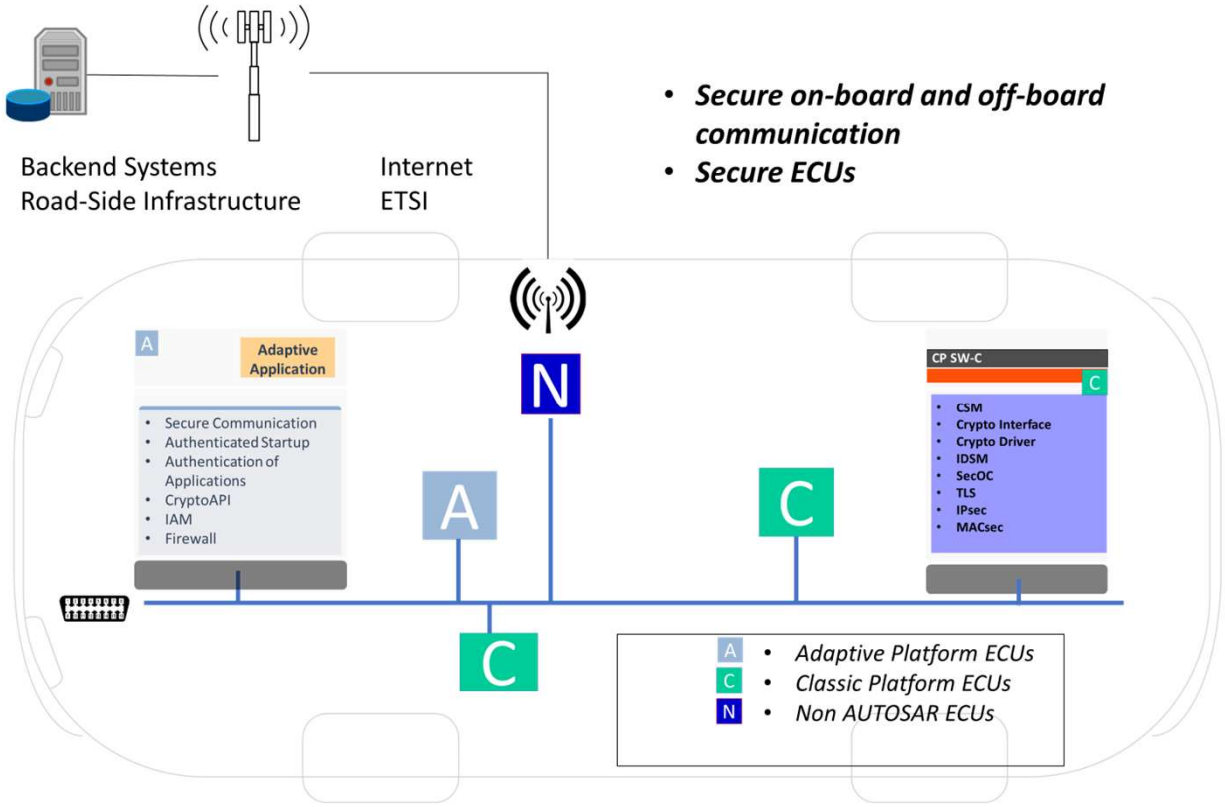
Intrusion Detection System, Firewall

**In vehicle network**

SecOC, (D)TLS, IPsec, MACsec

**Individual ECU**

Crypto API, Key Management, Identity and Access Management, Trusted Platform, Secure Update



# Deep dive Classic AUTOSAR Crypto Stack

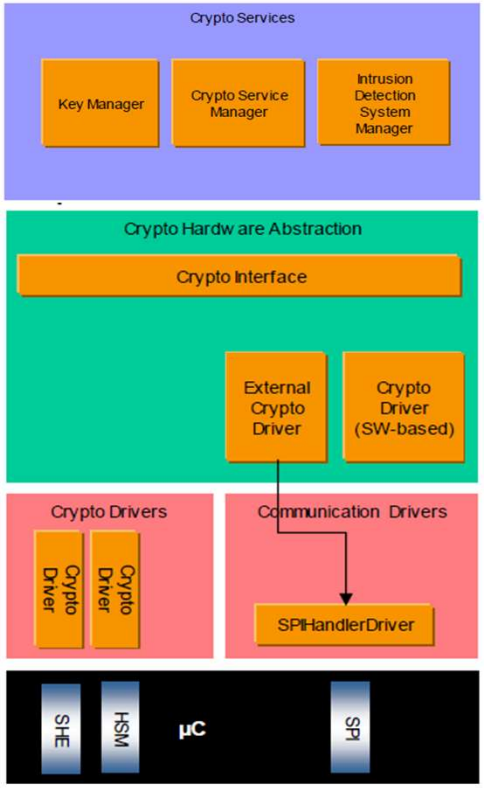
## Classic AUTOSAR Crypto Stack Architecture

**KeyM**
Certificate management, OEM key management support

**Crypto Service Manager**
Provides service layer access to cryptographic primitives and keys

**Crypto Interface**
Manages underlying crypto implementations and provides a uniform interface to upper layers

**Crypto Driver**
Implements the actual crypto primitives and key store (e.g. as SW lib or HSM)



# Deep dive Classic AUTOSAR Crypto Stack

## Classic AUTOSAR Crypto Stack Architecture

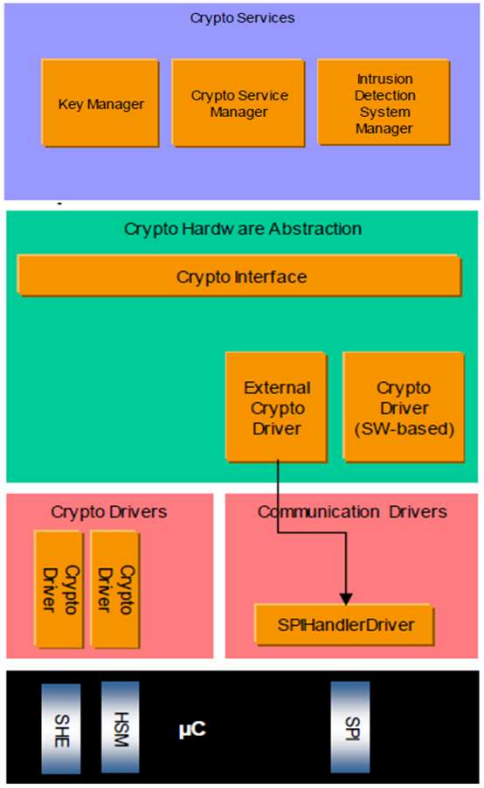
**Motivation for the layered architecture**

Support for multiple parallel crypto implementations on the ECU

- Support for multiple key/certificate stores (e.g. HSMs)
- Support for multiple crypto implementations (e.g. if special primitives are required for a use-case)

➔ Architecture allows to connect to external secure environments, like e.g. trusted execution environments

➔ AUTOSAR provides SW-specifications and does not impose requirements on the underlying hardware



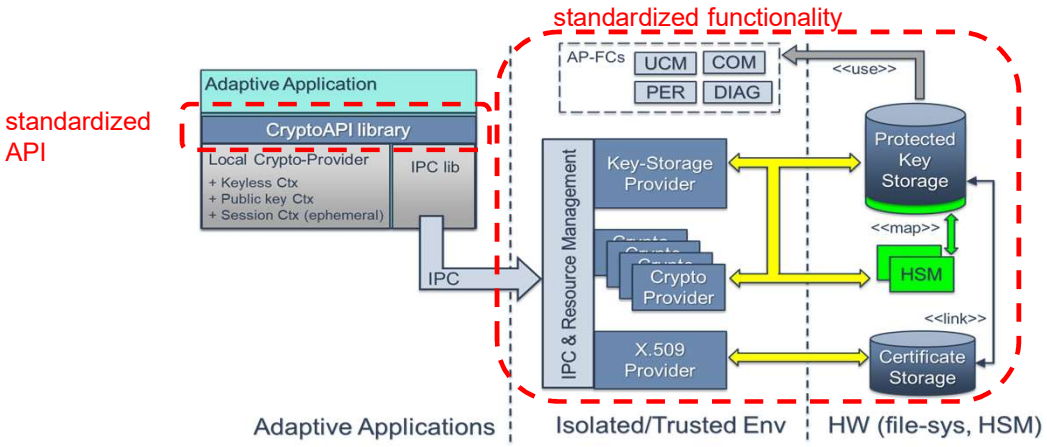
# Deep dive Adaptive AUTOSAR Crypto Stack

## Adaptive AUTOSAR Crypto Stack Architecture

Key Features

- Key management
- Cryptographic transformations
- Dedicated certificate support

**Standardized access** to crypto libraries allows implementation of custom crypto-services and easy extension of available primitives




**Secure use and management of key-material** from user space by separation of *user-interface* (library) and protected *stack service*

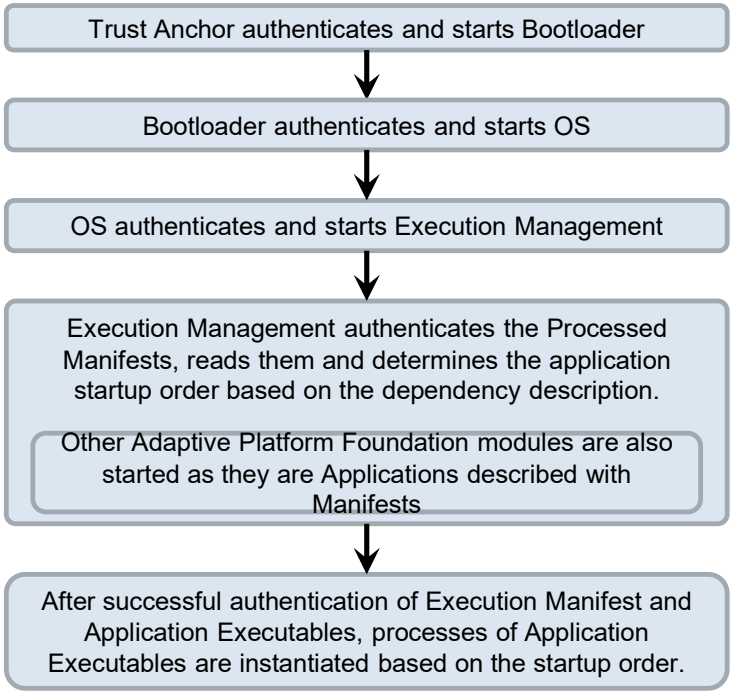
**Certificate management** including X.509, OCSP and CRL/delta-CRL

➔ Providers abstract underlying secure environment implementation (HSM, TPM, TEE, …)

# Authenticated Start-up

## Reliance on root of trust

- Ensure **authenticity** and **integrity** of running software
- Assumes a platform **"root of trust"**
- The trust is passed to **Execution Management** (chain of trust)
- Execution management is responsible for process creation and starting of processes based on processed manifests
- The start-up sequence will start after integrity and authenticity is ensured for :
  - Machine Manifest
  - Executable
  - Relates Process shared objects
  - Execution Manifest
  - Service Instance Manifest
- Two modes : **Monitoring** or **Strict**



# The AUTOSAR Opening Strategy

## A Set of Measures

- ✓ Regional Representations
- ✓ 3rd Party Collaboration
- ✓ Premium Partner Plus
- ✓ Derived Applications

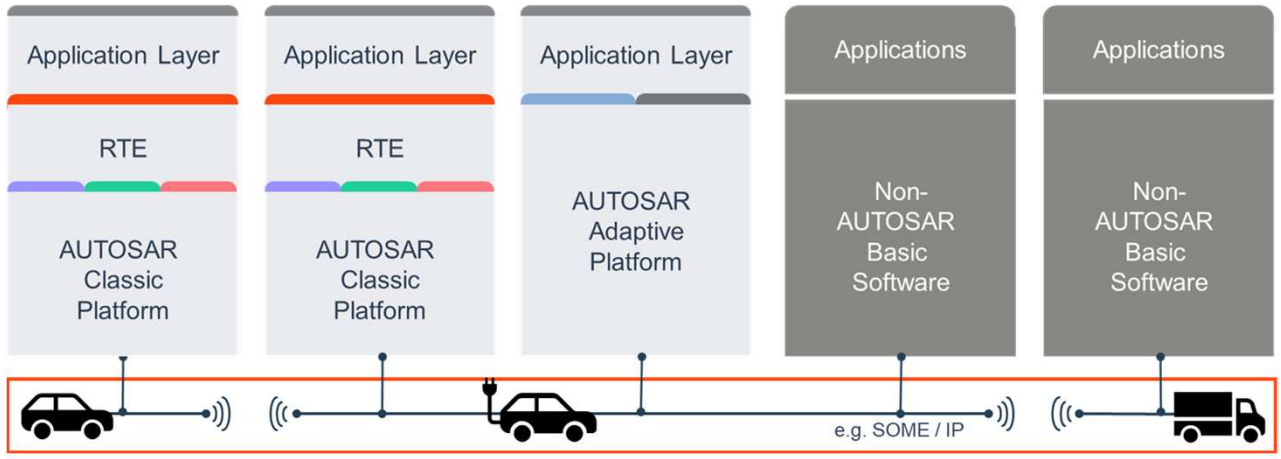

- Easier Access to a limited scope of AUTOSAR Work [in progress]
- Automotive API Project [in progress]

# The AUTOSAR Opening Strategy

## Software Defined Vehicle (SDV) - Easier Access

- **The new "Associate Partner Light" variant**
  - For free.
  - Exploitation rights for very limited scope of AUTOSAR standards.

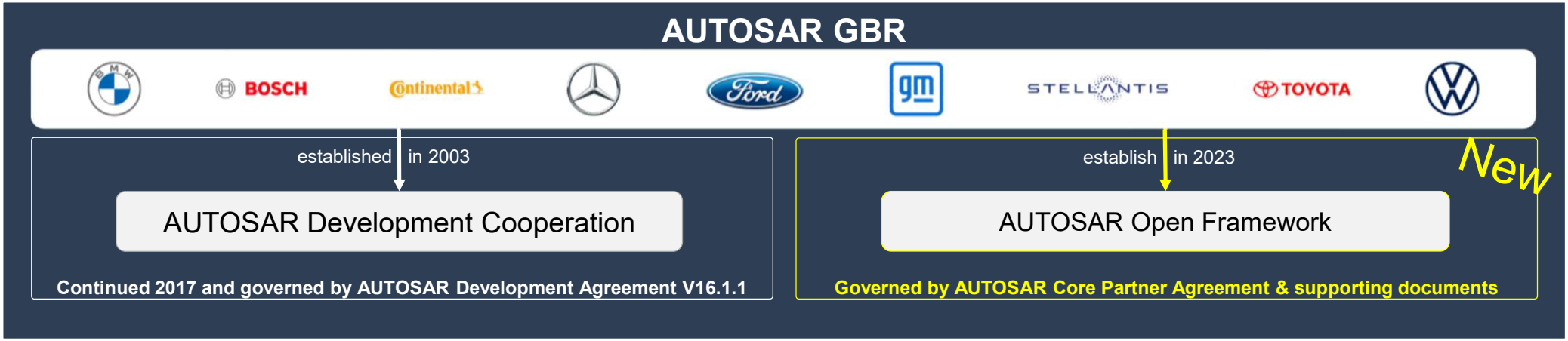
**Easier access to provide AUTOSAR compatible components or products**



# The AUTOSAR Opening Strategy

## Software Defined Vehicle (SDV) - Enable Collaboration

- **The new AUTOSAR Open Framework (AOF)**
  - to enable open collaboration in the SDV ecosystem **considering the overarching purpose of AUTOSAR**.
  - to **foster an ecosystem** of complementary standards, software implementations, and capabilities
  - to allow new activities **beyond the limits** of the AUTOSAR Development Cooperation.
  - is **open for interested parties** from the automotive and related industries to develop joint solutions.



# Big Picture

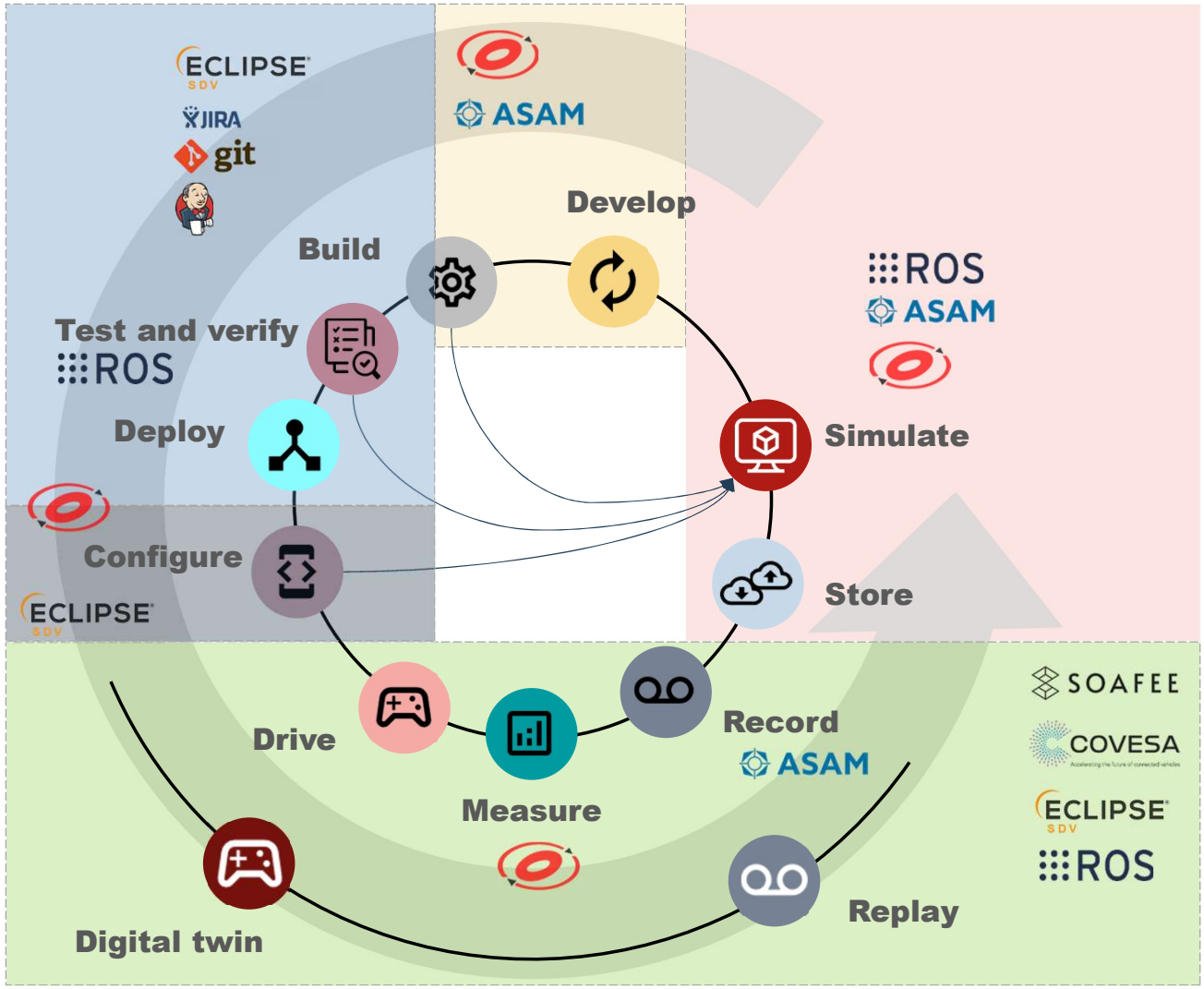
(selected stakeholder only)

ADAS
Development Cycle

The SDV Ecosystem is too huge for a single organization!

Each organization must find its role, position and interfaces in this development cycle.

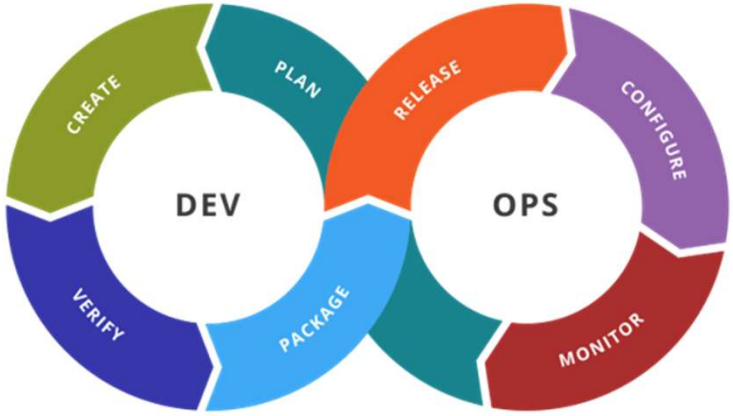
Compatibility is mandatory



# The Emergence of an Ecosystem

## Software Defined Vehicle (SDV) - Collaboration Between Multiple Stakeholders

A future automotive development environment will be provided by different organizations in an orchestrated collaboration.


*Exemplary excerpt

# The AUTOSAR Opening Strategy

## 3rd party Collaborations

- Dependable Backend Communication (VSS/SOVD) – with Covesa
- Dependable Demonstration with OpenX/OSI Standards – with ASAM
- Dependable Hardware Acceleration/ Parallelism concepts – with Khronos
- Rust language AUTOSAR Working Group activity – with MISRA
- Road vehicles — Qualification of pre-existing software products for safety-related applications – with ISO
- Road Vehicles — Safety and artificial intelligence – with ISO
- **Cybersecurity with GlobalPlatform**

# Global Platform / AUTOSAR collaboration

## Current status

- AUTOSAR WG-SEC and Global Platforms are currently evaluating possible collaboration scenarios
- Timeline
  - August 2nd: First joint session during AUTOSAR WG-SEC Face2Face
  - October 10th/11th: Follow-up joint session (planned)
- Take-aways & focus areas
  - Higher overlap with Adaptive AUTOSAR identified → Focus on this area
  - Deeper analysis if TEEs can also be used on µCs with Classic AUTOSAR
    - Examples: Cortex-M, Cortex-R

# Summary

- ✓ AUTOSAR offers a comprehensive software framework and a lot of building blocks for future dependable vehicle functions as part of future mobility solutions.
- ✓ The AUTOSAR platforms are compatible to each other and meet high demands for safety and cybersecurity.
- ✓ The AUTOSAR standard provides a sound basis for certification.
- ✓ AUTOSAR collaborates with GP for Cybersecurity features

# AUTOSAR Open Conference 2024

With the motto “Global Software Solutions for Future Mobility Challenges”, the **15th AUTOSAR Open Conference** will be held in **Tokyo, Japan on June 11th-12th, 2024.**

Please save the date for the 15th AOC and stay tuned for more information on AUTOSAR Web site.


AUTOSAR™
Thank you!
BOSCH
Continental
Ford
gm
STELLANTIS
TOYOTA
VOLKSWAGEN GROUP