Introduction of AUTOSAR R23-11

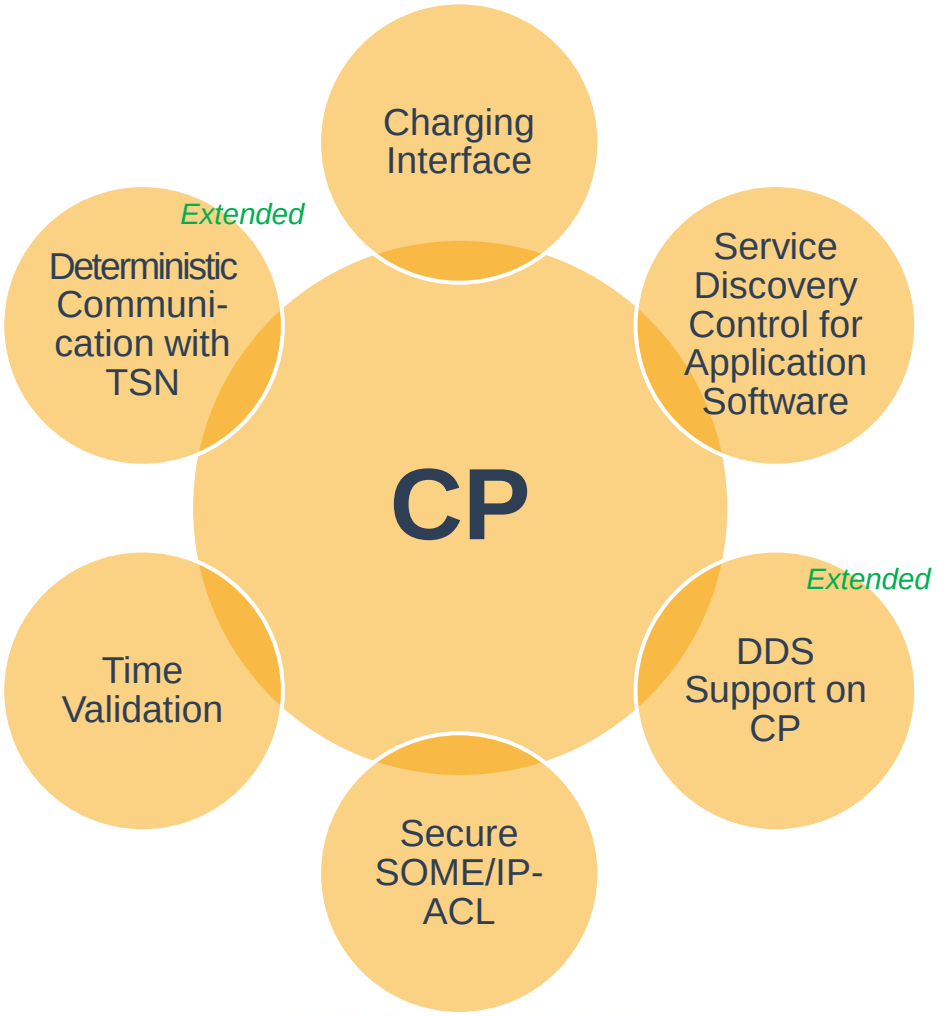
Qian Jiamin

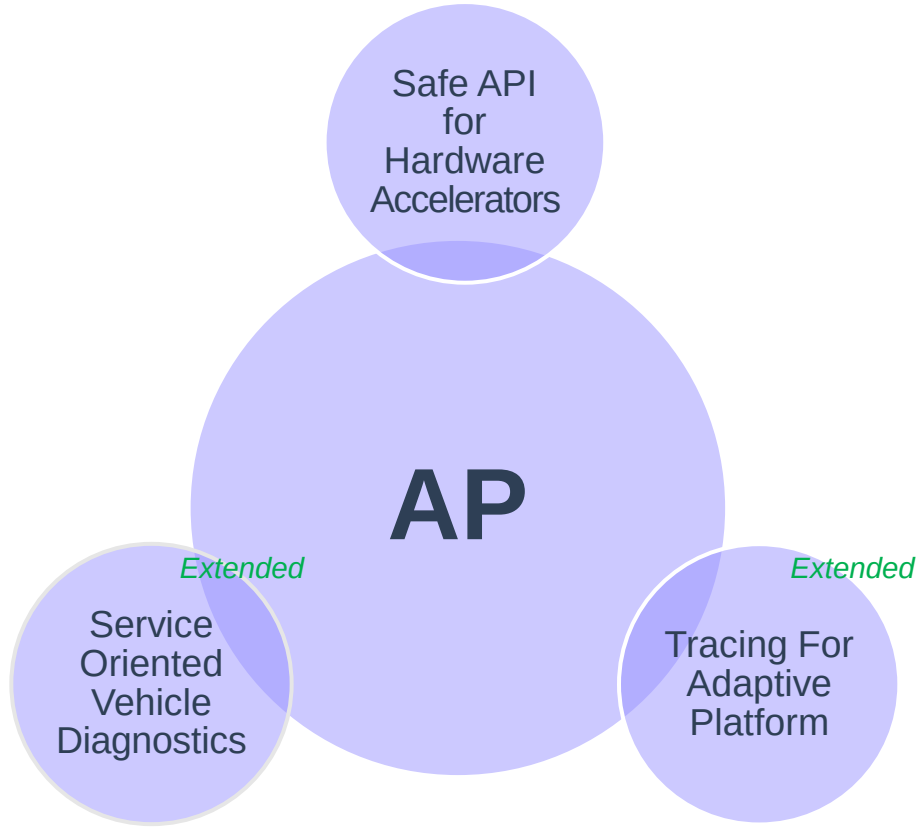
AUTOSAR China day

14 Mar 2024

BOSCH Continental Ford gm STELLANTIS TOYOTA VOLKSWAGEN GROUP

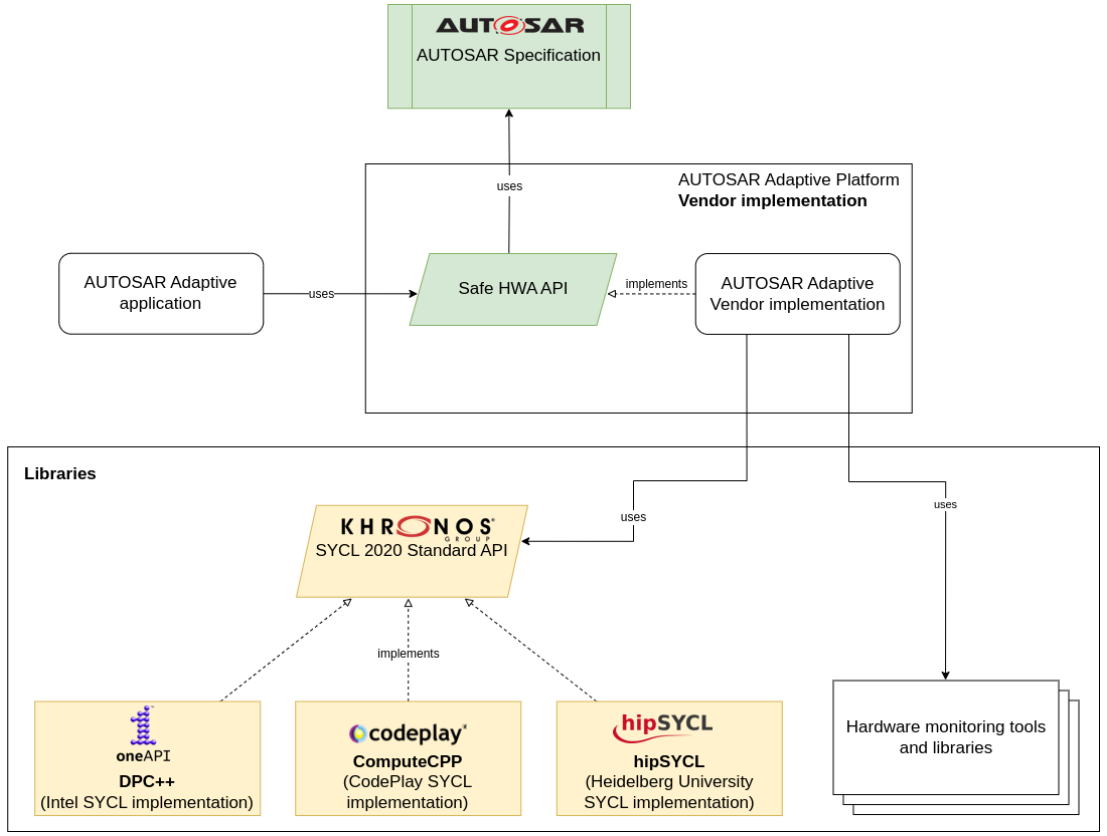
AUTOSAR Release R23-11 – Concepts Overview





Safe API for HW Accelerator

Architecture



The code is supplied by the vendor of ECU knowing its HWA features best.

Safe API for HW Accelerator

Functionality

- Data storage and management:
  - We have big sets of data
  - That must be stored safe AND efficiently for computing
- Task execution:
  - Queueing
  - Event and error handling
- Device management and monitoring:
  - Abstraction of HWA
  - Provide status (healthy, unhealthy, high load …)
- Runtime configuration:
  - Configuration of HWA resources according to machine manifest

Time Validation

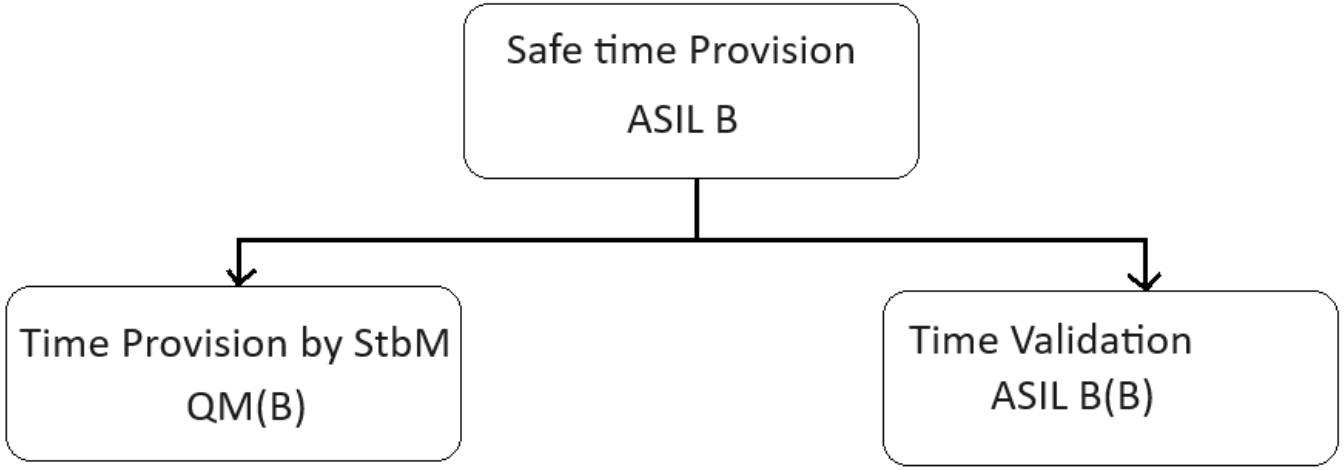
Topic

- Many sensor values are only valid with a valid time stamp.
- If one value depends on several values from different ECU then these values should be taken at the same time.
- If this value is safety relevant then it shall be computed on the base of safe inputs.
- Also a safe time value.
- AUTOSAR offers a time value. How to make it a safe time value?

Time Validation

Functionality

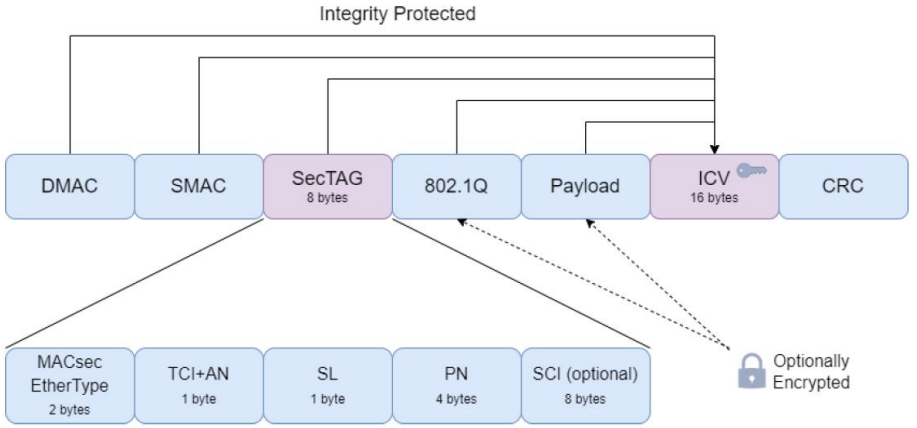
An ECU shall have a local instance of a global time in ASIL B quality.



The ASIL B step is done with a HW timer, independent from StbM.

MACsec

- MACsec is a secure communication protocol on Data Link Layer
- All higher-level protocols (IP, TCP, …) are protected with MACsec
- MACsec operates on a low layer, utilizing HW accelaration feature for high throughput
- MACsec operates too close to the HW for a detailed specification in Adaptive AUTOSAR
- New document AP_EXP_MACsec provides guidelines how to use MACsec with Adaptive AUTOSAR



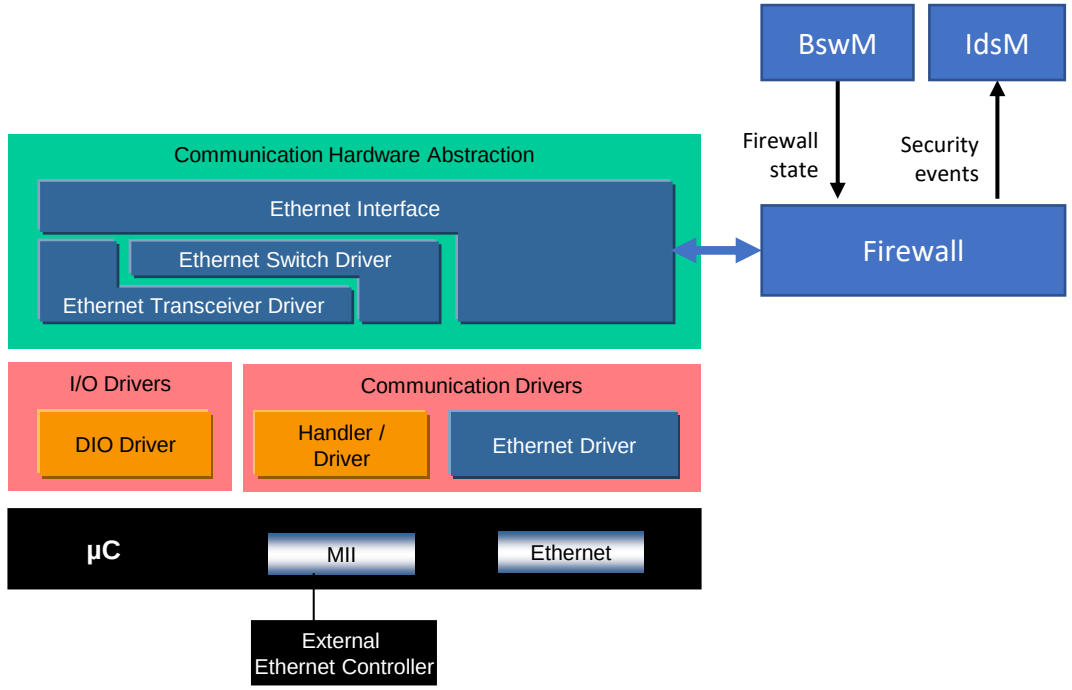
AUTOSAR

Explanation of MACsec and MKA Protocols implementation and configuration guidelines
AUTOSAR AP R23-11

Document Title	Explanation of MACsec and MKA Protocols implementation and configuration guidelines
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	1067
Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R23-11

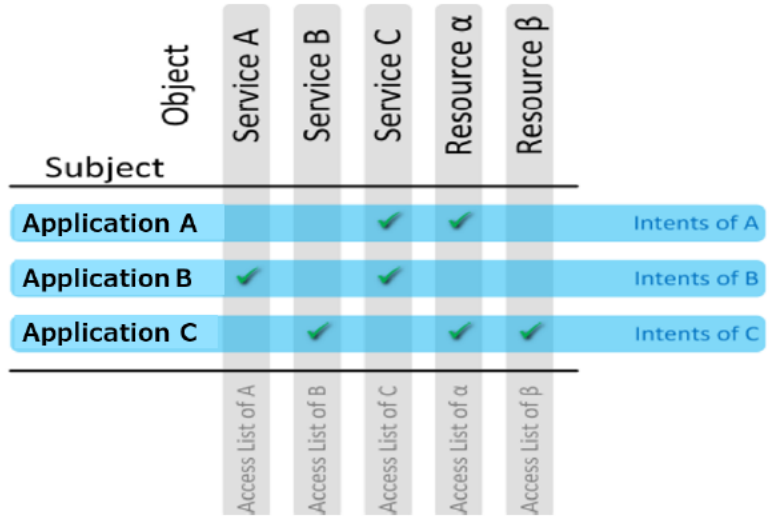
Firewall

- Protects ECU by filtering unwanted Ethernet communication
- Supports stateless filtering, stateful filtering and deep packet inspection (SOME/IP, DoIP, DDS, generic)
- Firewall for CP (R23-11) has the same goal/use-cases as Firewall for AP (R22-11) + Firewall on switches
- Configuration of firewall rules via ARXML



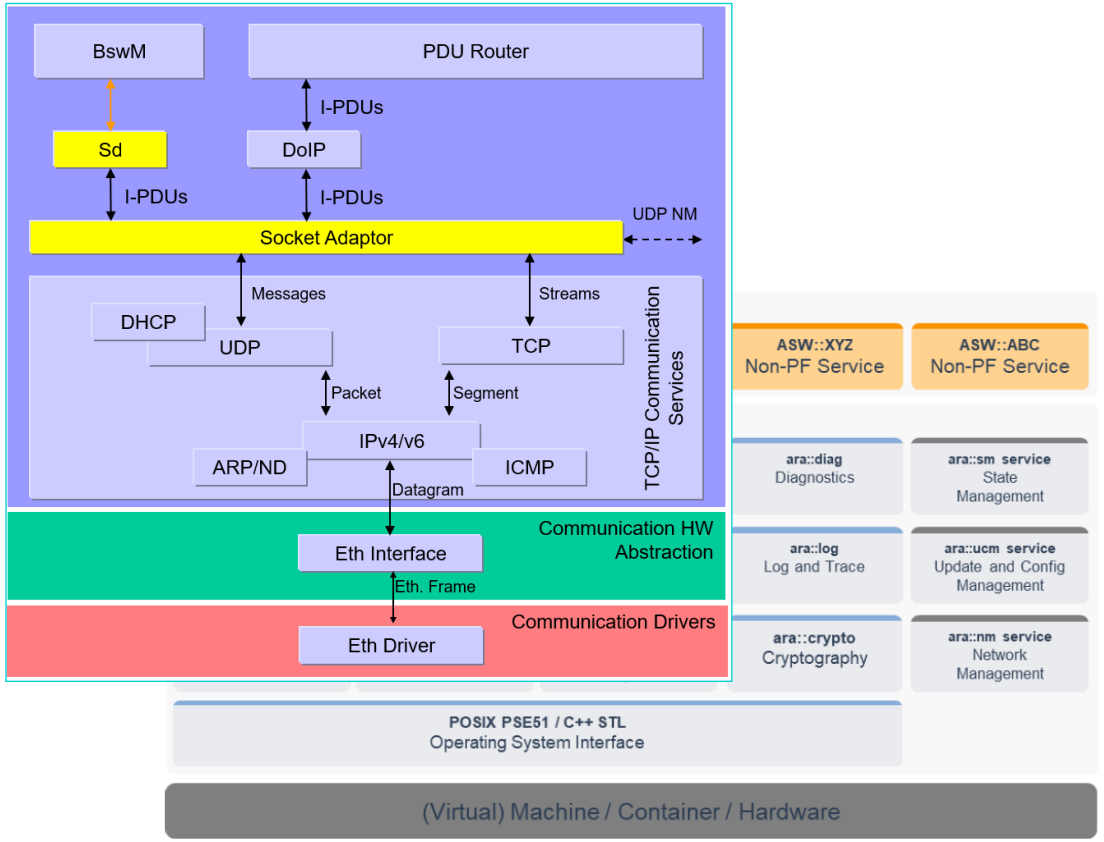
Introduction of EXP_IAM

- AUTOSAR Identity & Access Management protects services and resources from unauthorized use in Adaptive
- The IAM specification is distributed among many documents
  - Policy enforcement in functional cluster specification
  - IAM configuration in AP_TPS_ManifestSpecification
  - SWS_IdentityAndAccessManagement: Mostly explanatory, not much specification
- IAM specification can be confusing due to its distributed specification
- With R23-11, SWS_IAM has been replaced with EXP_IAM to give a clear picture of the feature



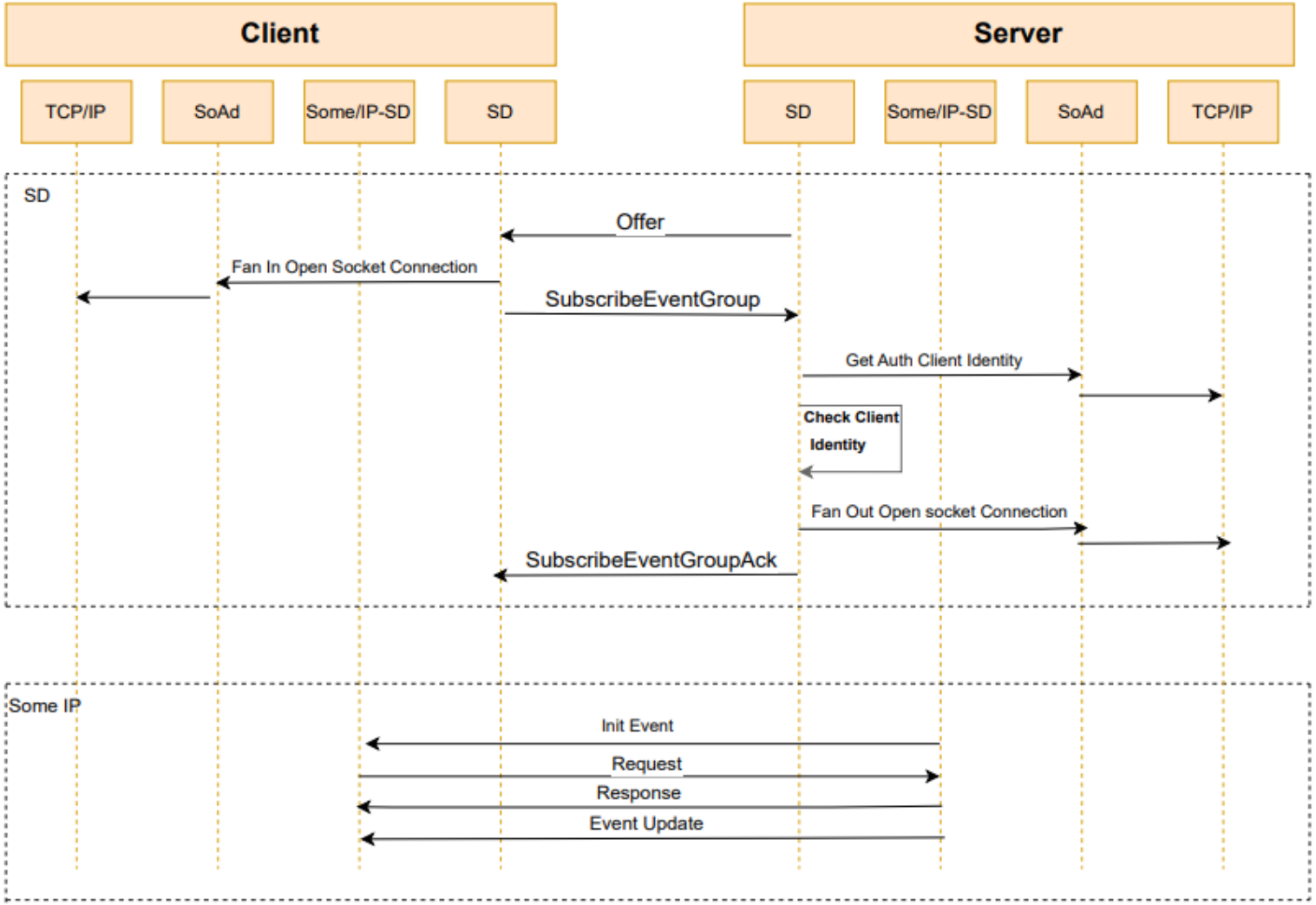
Secure SOME/IP-ACL

This concept introduces the possibility of limiting the Ethernet communication “SOME/IP” from known permitted listed authenticated communication partners to specific service instance, so secured service instance can only be accessed (Offered, Subscribed, or Consumed) by defined partners.



Secure SOME/IP-ACL

Client/Server Subscription Sequence “Classic Platform” with ACL check injected



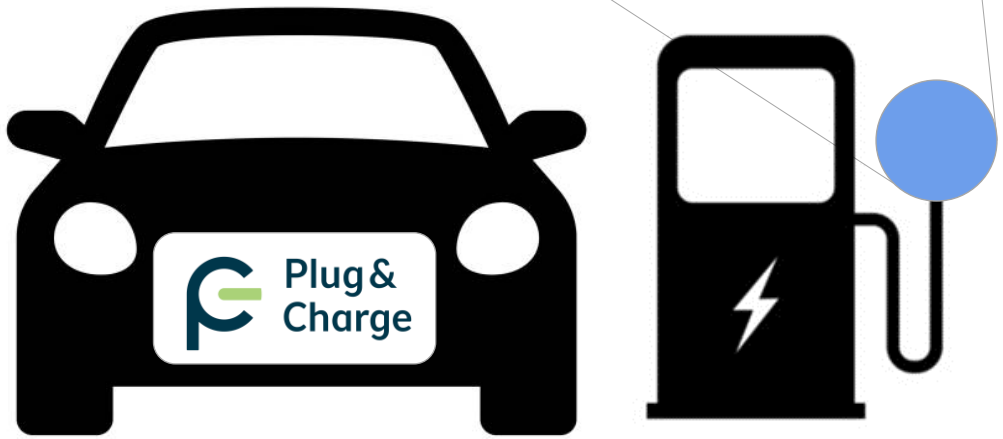
Charging Interface

Motivation

To support the e-mobility, the worldwide established charging infrastructure shall be supported by AUTOSAR according to the ISO 15118-2:2014.

- AC & DC charging.
- EIM (external identification means) & PnC (plug and charge).
- Digital communication between electric vehicle EV and EVSE (electric vehicle supply equipment) as per ISO-15118-2/20.
- Supported by the AUTOSAR Classic Platform.
- Charging over Ethernet protocol.

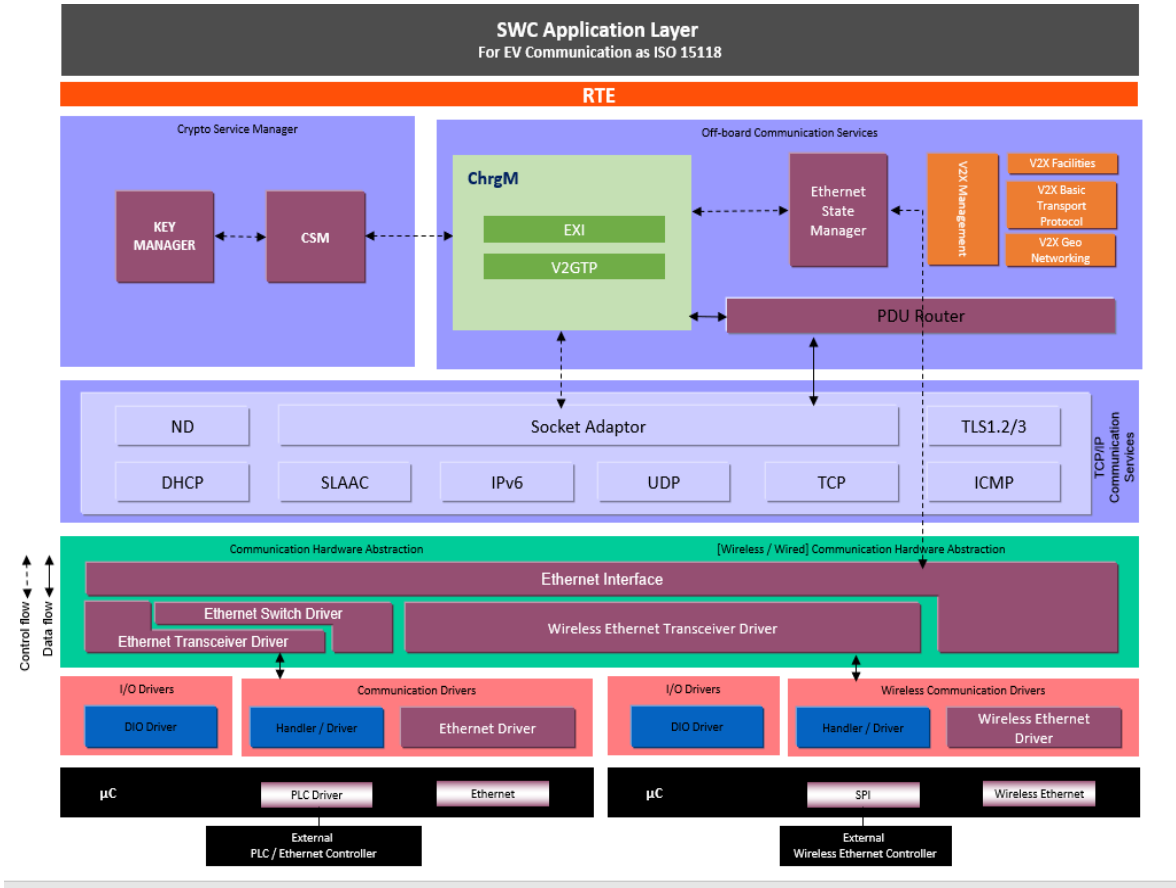
Current type and plug name	Region			
	Japon	China	America	Europe
AC				
Plug name	Type 1 - J1772	GB/T	Type 1 - J1772	Type 2
DC				
Plug name	CHAdeMO	GB/T	CCS - Type 1	CCS - Type 2



Charging Interface

Charging Manager (ChrgM)

- ChrgM will be a part of Communication Services and will communicate with other AUTOSAR modules to support the charging process.
- ChrgM will control the charging process using set of messages “V2G Message” given in the standard ISO15118-2:2014.
- The EXI (efficient XML interchange) is responsible for compression of the XML data for faster processing.
- the V2GTP (vehicle to grid transport protocol) defines the structure of the PDU, which is the header and payload definitions.



Service Discovery Control for Application Software

Motivation

Service Oriented Communication on classic platform is today typically used with “auto offer / auto subscribe” where SD is performed during startup phase of all ECUs.

If Application Software does not need Service Oriented Communication from the start, it shall be possible to trigger Service Discovery by the Application at any point in time – both for Server and Clients.

User Benefit

Control Service Discovery functionality by Well defined Interface and Behavior of the BswM for Service Oriented Communication.

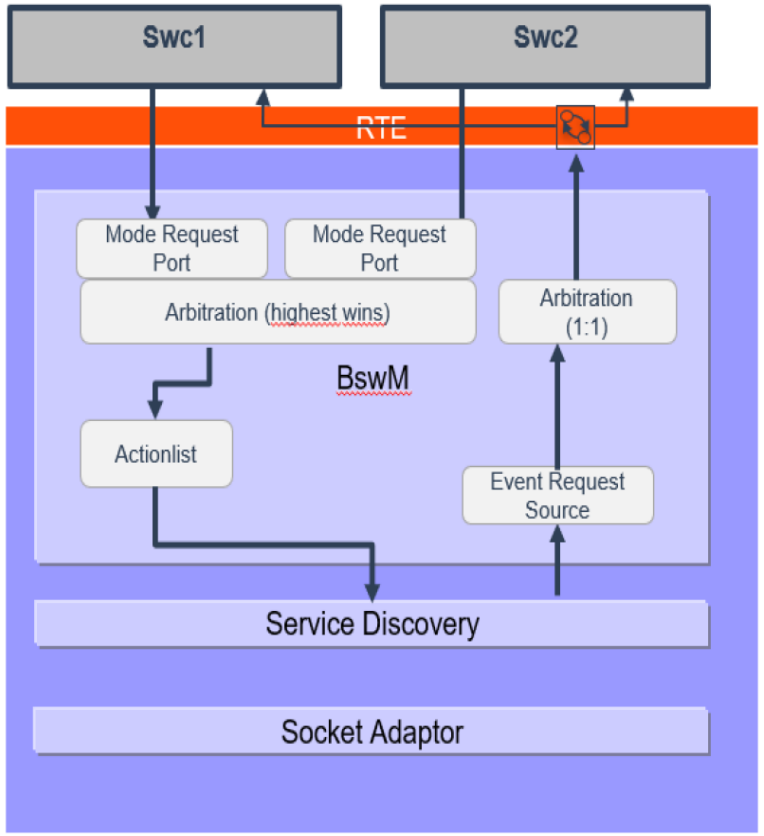
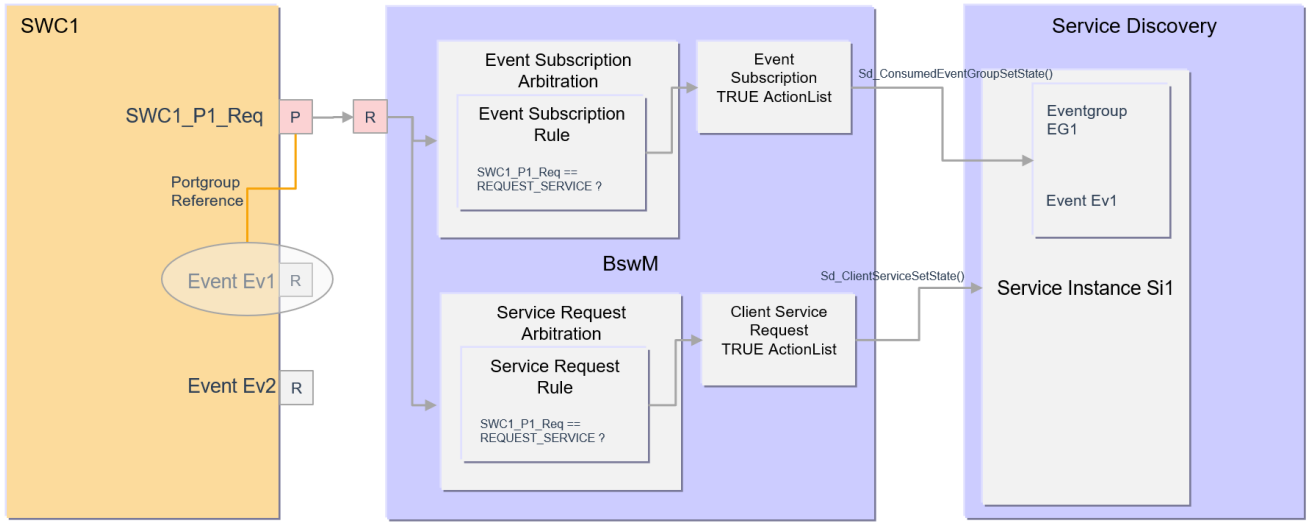


Figure 3.3: Service Discovery Control Flow Overview

Service Discovery Control for Application Software

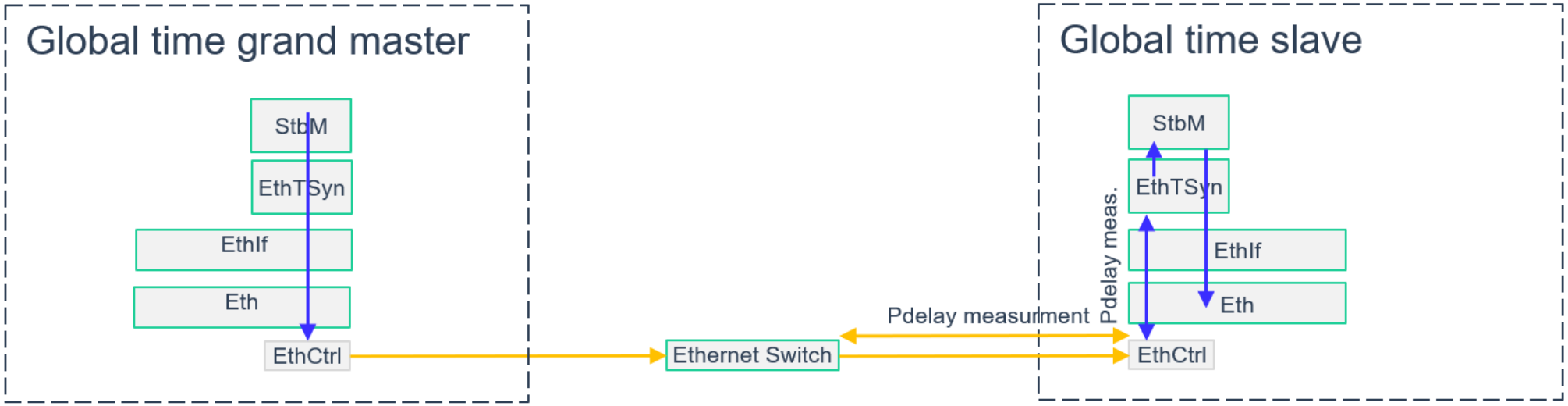
Use Cases

- A Software Component in Service Server Offer / Stop-Offer the Service.
- Service Server checks whether there are any subscribers of his offered service.
- Service Client subscribes to a Service.
- Service Client checks whether the subscription was successful.

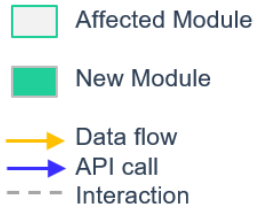


Deterministic Communication with TSN

Extensions to Enhance Precision for Global Time Synchronization

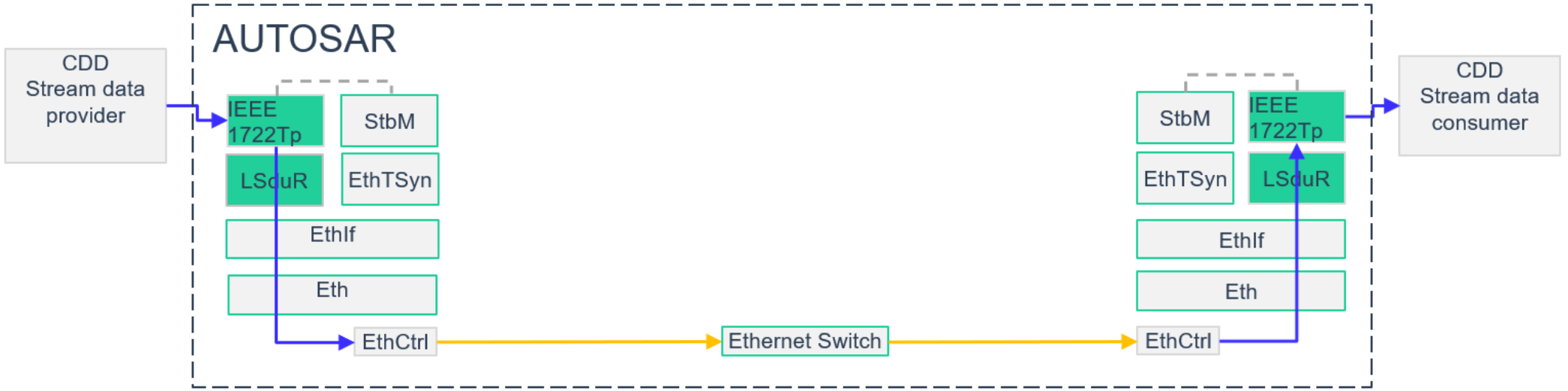


- Support neighbour rate ratio calculation specified by IEEE802.1AS-2022
- Support configuration of up to two hardware clocks
  - PTP (Precision Time Protocol) hardware clock, with adjustable offset and rate
  - free running hardware clock
- Support configuration of PPS (Pulse Per Second) signal generation to validate quality of synchronized global time



Deterministic Communication with TSN

IEEE 1722 Audio/Video Transport Protocol - Stream Handling



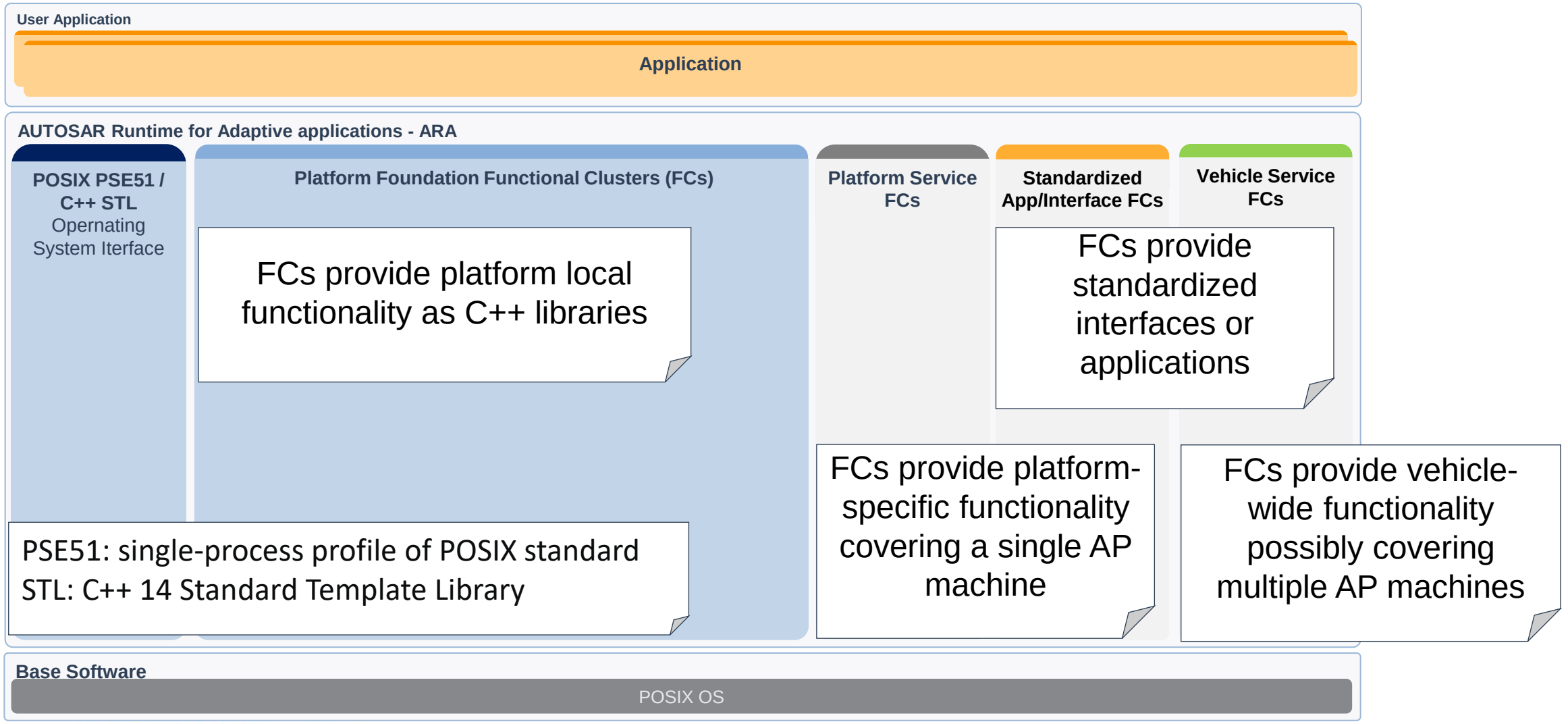
- Support transmission and reception of IEEE1722 streams
  - Audio and video streams: AAF (AVTP Audio Format), 61883_IIDC, RVF (Raw Video Format)
  - Control streams: CRF (Clock Reference Format), TSCF (Time Sensitive Control Format), NTSCF
- Extend Ethernet Switch Driver to support the following features:
  - passive stream identification specified by IEEE802.1CB
  - Per-Stream Filtering and Policing specified by IEEE802.1Q-2022
  - extension of Credit Based Shaper, introduction of Asynchronous Traffic Shaper
- Introduce HW supported data transfer (e.g. DMA) for efficient handling of large data transfer

What is the Adaptive Platform all about?

Mixed-critical automotive extension to POSIX

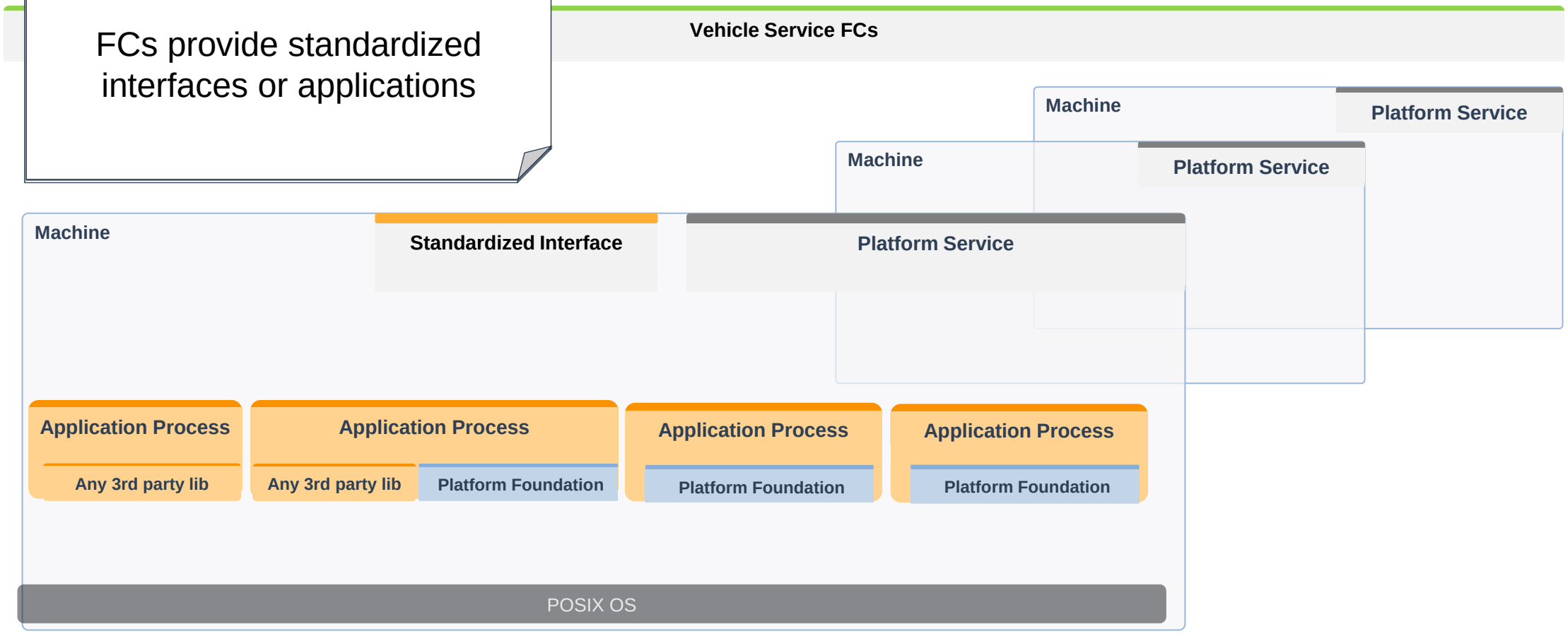
- Standard automotive connectivity
- Automotive-specific functional add-ons
- Functional Safety and Cyber Security
- E/E Architecture development
  - Top-Down Workflow for distributed development
  - Formal exchange formats

Logical Architecture View - overview

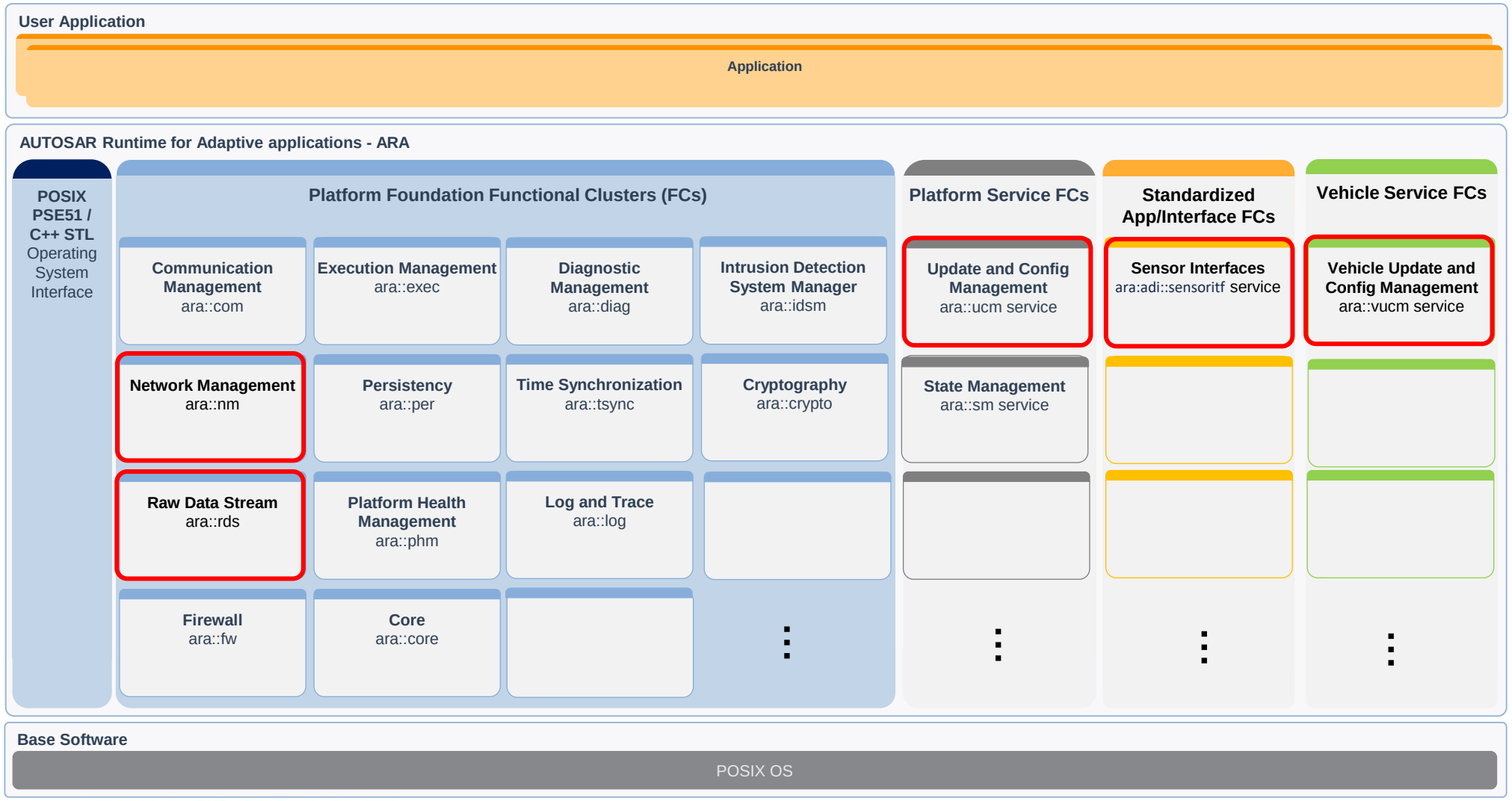


Logical Architecture View - overview

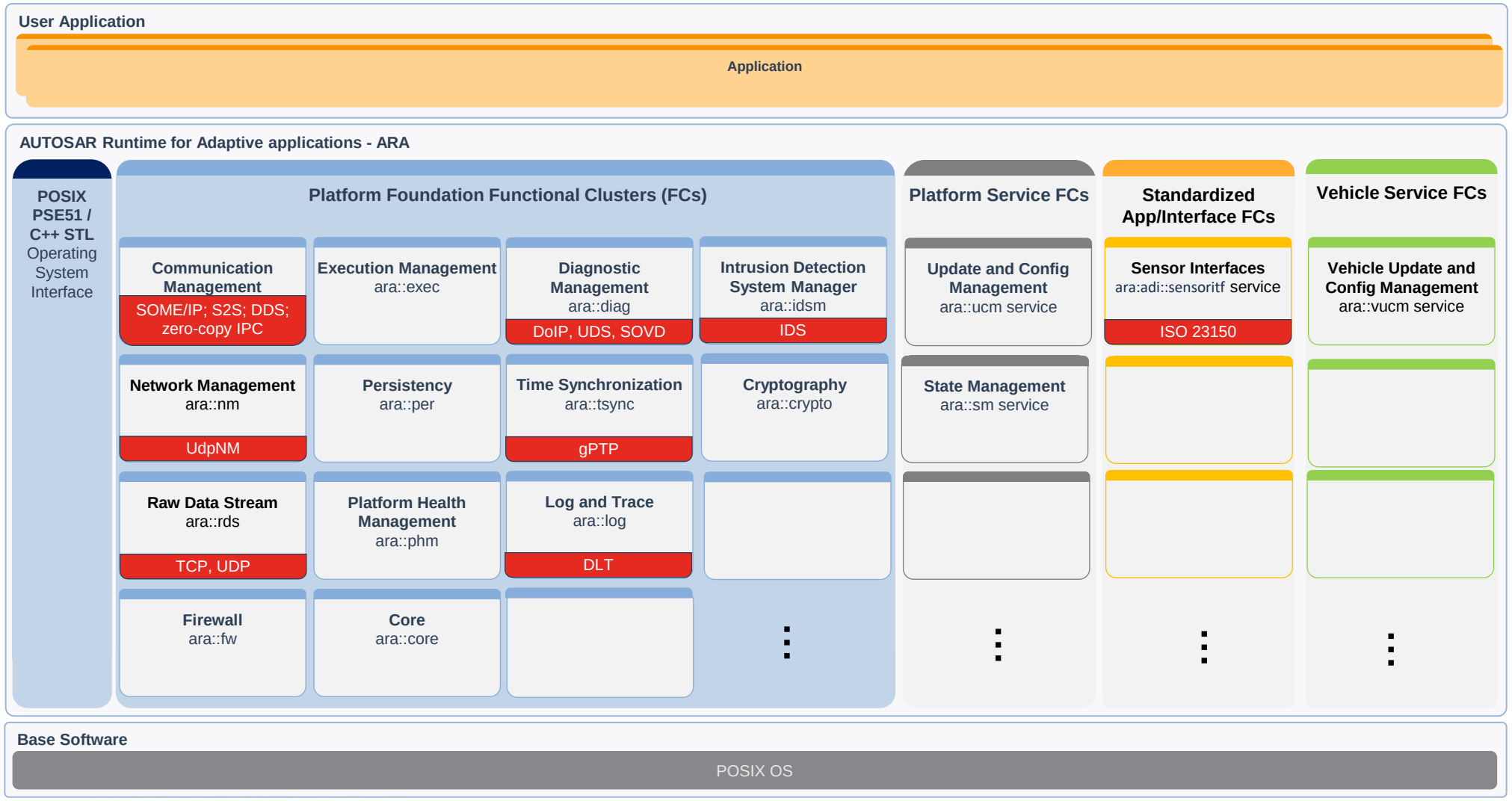
FCs provide standardized interfaces or applications



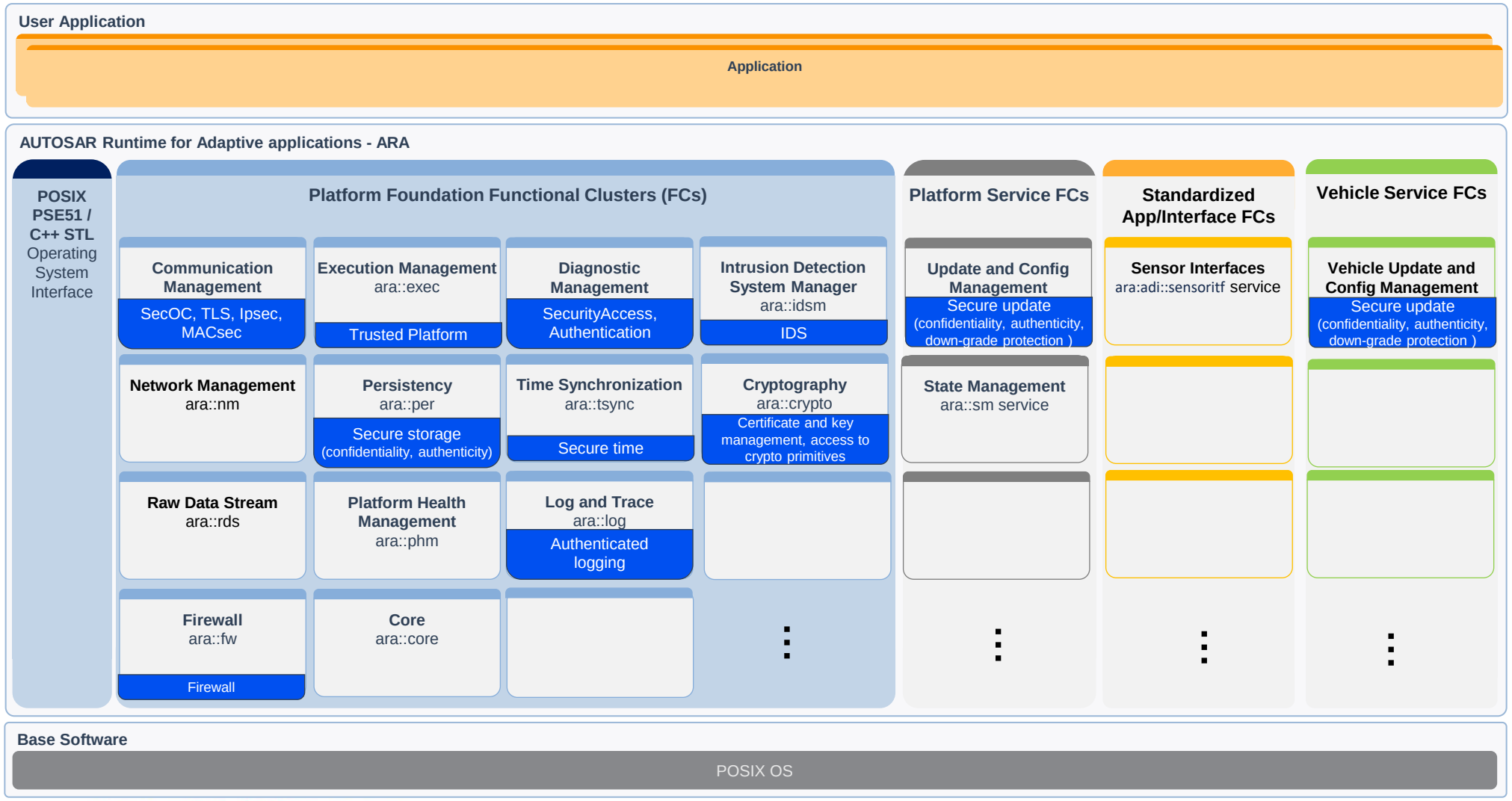
Logical Architecture View - base



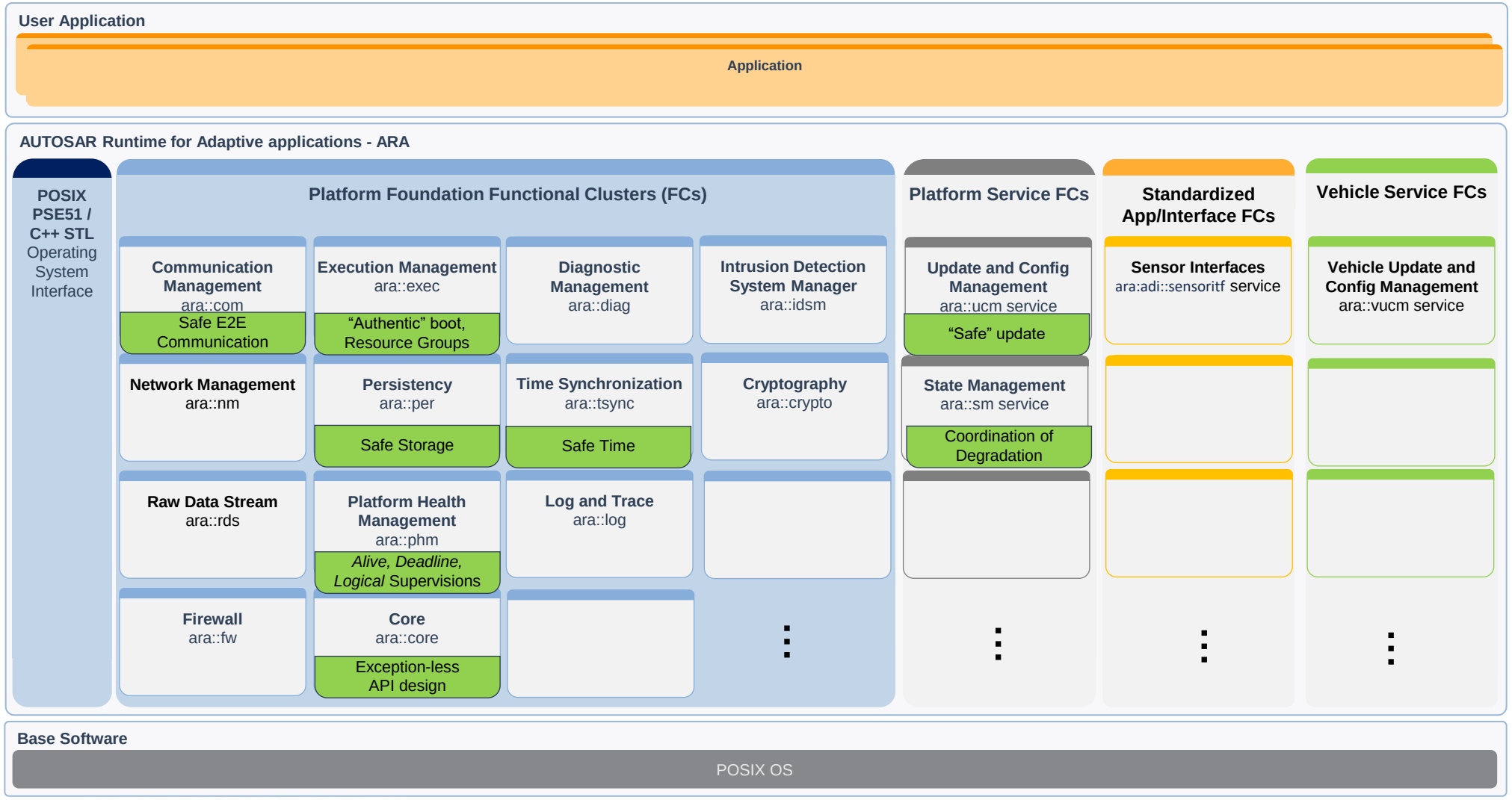
Logical Architecture View - protocols



Logical Architecture View - security



Logical Architecture View – safety



AUTOSAR Release R23-11 in numbers

1726	Incorporation Tasks in all 3 AUTOSAR Standards
1245	Discussed Change Requests within the AUTOSAR community
198	AUTOSAR Partner collaborating in 20 Working Groups
328.757	Adaptive Platform code lines to demonstrate and validate the Adaptive Platform standard
11	New Concepts for Adaptive and Classic Platform to tackle future goals
2	Standardized AUTOSAR Software Platforms to
1	Define one holistic E/E System Architecture for Future Intelligent Mobility

BOSCH Continental Ford gm STELLANTIS TOYOTA VOLKSWAGEN GROUP

Thanks a lot for your attention!
Enjoy the coming deep dives.

BMW · Hyundai · BOSCH · Continental · Ford · gm · Mercedes-Benz · STELLANTIS · TOYOTA · VOLKSWAGEN GROUP